

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-59323

(P2000-59323A)

(43) 公開日 平成12年2月25日 (2000.2.25)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
H 0 4 H 1/00		H 0 4 H 1/00	F
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 B
9/10			6 2 1
29/08		13/00	3 0 7 Z
H 0 4 N 7/167		H 0 4 N 7/167	Z
審査請求 未請求 請求項の数43 O L (全 28 頁)			

(21) 出願番号 特願平10-224825

(22) 出願日 平成10年8月7日 (1998.8.7)

(31) 優先権主張番号 特願平10-31847

(32) 優先日 平成10年2月13日 (1998.2.13)

(33) 優先権主張国 日本 (J P)

(31) 優先権主張番号 特願平10-151586

(32) 優先日 平成10年6月1日 (1998.6.1)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72) 発明者 西村 拓也
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 飯塚 裕之
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100092794
弁理士 松田 正道

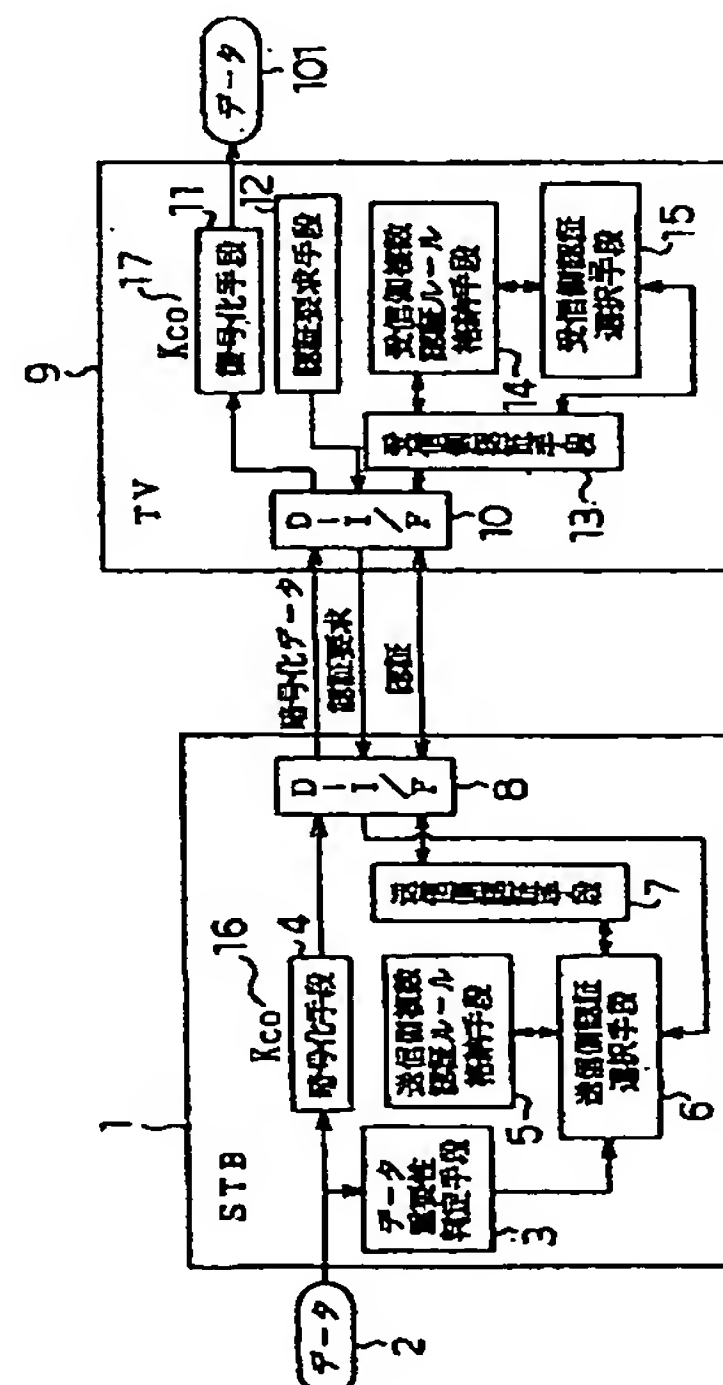
最終頁に続く

(54) 【発明の名称】 デジタルAVデータ送信ユニット、デジタルAVデータ受信ユニット及び、デジタルAVデータ送受信システム、媒体

(57) 【要約】

【課題】 重要でないデータの認証に多くの時間を要したり、重要なデータであるにもかかわらずその認証が偽造や改竄に弱い。また、ユニットによって認証に必要な厳密さが異なる。

【解決手段】 データ2の重要度を判定するデータ重要性判定手段3、その判定結果に基づき送信側複数認証ルール格納手段5から一種類のルールを選択する送信側認証選択手段6及び、その選択された認証ルールに基づき認証を行う送信側認証手段7を有するSTB1と、認証要求を行う認証要求手段12、送信側で選択された認証ルールと同じ認証ルールを受信側複数認証ルール格納手段14から選択する受信側認証選択手段15及び、その選択された認証ルールに基づき認証を行う受信側認証手段13を有するTV9とを備える。



【特許請求の範囲】

【請求項1】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニット。

【請求項2】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAVデータ送信ユニットを通信の対象とし、前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ受信ユニット。

【請求項3】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルAVデータ受信ユニットとを備えたことを特徴とするデジタルAVデータ送受信システム。

【請求項4】 デジタルAVデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、前記データ重要性判定手段の判定結果に基づき、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照

決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニット。

【請求項5】 前記送信ユニットは前記受信ユニットの各機能を有し、前記受信ユニットは前記送信ユニットの各機能を有することを特徴とする請求項3記載のデジタルAVデータ送受信システム。

【請求項6】 前記受信ユニットの機能を有する送信ユニット、あるいは前記送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルAVデータを互いにやりとりできることを特徴とする請求項5記載のデジタルAVデータ送受信システム。

【請求項7】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも備えたデジタルAV送信ユニット。

【請求項8】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットを通信の対象とし、前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ受信ユニット。

【請求項9】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記デジタルAVデータ受信ユニットが有する認証ルールを、前記送信側複数認証ル

ール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき前記認証を行う送信側認証手段とを少なくとも有するデジタルＡＶ送信ユニットと、前記認証の要求を行う認証要求手段と、自らの一種類の前記認証ルールを格納する受信側認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１０】 所定の管理基準を格納した管理基準格納手段と、デジタルＡＶデータ受信ユニットから認証要求を受けて、そのデジタルＡＶデータ受信ユニットの種類又は重要度に応じて、前記管理基準格納手段の前記管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って前記管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたことを特徴とするデジタルＡＶ送信ユニット。

【請求項１１】 前記管理基準は、不正な、あるいは正当なデジタルＡＶデータ受信ユニットを識別できる基準リスト（ＣＲＬ）であることを特徴とする請求項４又は１０に記載のデジタルＡＶ送信ユニット。

【請求項１２】 前記送信ユニットに、前記受信ユニットが二つ以上接続され、前記送信ユニットとの間で、デジタルＡＶデータをやりとりできることを特徴とする請求項９記載のデジタルＡＶデータ送受信システム。

【請求項１３】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルＡＶデータ送信ユニット。

【請求項１４】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルＡＶデータの重要度を判定するデータ重要性判定手段と、前記データ重要性判定手段の判定結果に基づき、前記送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信

側認証選択手段と、単一認証デジタルＡＶデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、前記ユニット認証ルール情報受信手段で受信された前記認証ルールについての情報に基づき、前記単一認証デジタルＡＶデータ受信ユニットが有する認証ルールを、前記送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、前記送信側認証選択手段又は前記送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルＡＶデータ送信ユニットと、

前記認証の要求を行う認証要求手段と、前記送信側認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを前記受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で前記選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルＡＶデータ受信ユニットと、認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、前記認証ルールについての情報を送信する認証ルール情報送信手段と、前記デジタルＡＶデータ送信ユニットとの間で前記認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルＡＶデータ受信ユニットと、を備えたことを特徴とするデジタルＡＶデータ送受信システム。

【請求項１５】 前記複数認証デジタルＡＶデータ受信ユニットは前記デジタルＡＶデータ送信ユニットの各機能を有し、前記デジタルＡＶデータ送信ユニットは前記複数認証デジタルＡＶデータ受信ユニットの各機能を有することを特徴とする請求項１４記載のデジタルＡＶデータ送受信システム。

【請求項１６】 前記複数認証デジタルＡＶデータ受信ユニットの各機能を有するデジタルＡＶデータ送信ユニット、あるいは前記デジタルＡＶデータ送信ユニットの機能を有する複数認証デジタルＡＶデータ受信ユニットが二つ以上互いに接続され、且つ、前記単一認証デジタルＡＶデータ受信ユニットが二つ以上接続され、デジタルＡＶデータを互いにやりとりできることを特徴とする請求項１５記載のデジタルＡＶデータ送受信システム。

【請求項１７】 デジタルＡＶデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルＡＶデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルＡＶデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等及びそれ以下のレベルの前記解読情報を、前記受信ユニットに送信

10

20

30

40

50

する解読情報選択手段とを備えたことを特徴とする送信ユニット。

【請求項18】 データの重要度に応じた複数のレベルで暗号化されたデジタルAVデータを送信する送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等及びそれ以下のレベルの前記暗号化データに対する解読情報を、前記送信ユニットに要求する解読情報要求手段とを備えたことを

特徴とする受信ユニット。

【請求項19】 デジタルAVデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルAVデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルAVデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等及びそれ以下のレベルの前記解読情報を、前記受信ユニットに送信する解読情報選択手段とを有する送信ユニットと、その送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等及びそれ以下のレベルの解読情報を、前記送信ユニットに要求する解読情報要求手段とを有する受信ユニットとを備えたことを特徴とするデジタルAVデータ送受信システム。

【請求項20】 デジタルAVデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルAVデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルAVデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等またはそれ以下のレベルの解読情報を前記受信ユニットに送信する解読情報選択手段とを備え、前記解読情報選択手段は、次に前記受信ユニットから解読情報の要求があった時に、その要求が前記判定済みの認証レベルと同等あるいはそれ以下のレベルの前記解読情報の場合は、前記認証手続きを行わずに要求された解読情報を前記受信ユニットに送信することを特徴とする送信ユニット。

【請求項21】 データの重要度に応じた複数のレベルで暗号化されたデジタルAVデータを送信する送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等またはそれ以下の

レベルの前記暗号化データに対する解読情報を前記送信ユニットに要求する解読情報要求手段とを備え、前記解読情報要求手段は、前記認証のレベルと同等あるいはそれ以下のレベルの解読情報を前記送信ユニットに要求する時は、前記認証要求を行わずに、前記解読情報の要求を行うことを特徴とする受信ユニット。

【請求項22】 デジタルAVデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、前記暗号化されたデジタルAVデータを受信する受信ユニットから要求された認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、前記受信ユニットからの、前記暗号化されたデジタルAVデータを解読するための解読情報の要求に対して、前記判定済みの認証レベルと同等またはそれ以下のレベルの解読情報を前記受信ユニットに送信する解読情報選択手段とを有し、前記解読情報選択手段は、次に前記受信ユニットから解読情報の要求があった時に、その要求が前記判定済みの認証レベルと同等あるいはそれ以下のレベルの前記解読情報の場合は、前記認証手続きを行わずに要求された解読情報を前記受信ユニットに送信する送信ユニットと、その送信ユニットから受信する暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を前記送信ユニットに要求する認証手段と、前記認証レベルと同等またはそれ以下のレベルの解読情報を前記送信ユニットに要求する解読情報要求手段とを備え、前記解読情報要求手段は、前記認証のレベルと同等あるいはそれ以下のレベルの解読情報を前記送信ユニットに要求する時は、前記認証要求を行わずに、前記解読情報の要求を行う受信ユニットとを備えたことを特徴とするデジタルAVデータ送受信システム。

【請求項23】 受信側ユニットから送られてきた認証要求について、認証を行い、又、その認証のレベルを判定し、そのレベルと同等な認証方法及びそれより低いレベルの認証方法に対応する暗号化方法のそれぞれの解読情報を、前記受信側ユニットからの解読情報の要求に応じて、前記受信側ユニットへ送信することを特徴とするデジタルAVデータ送信方法。

【請求項24】 受信側ユニットから送られてきた解読情報要求について、その要求された解読情報に対応する認証のレベルを判定し、そのレベルと前記受信側ユニットとの間で過去に実行した認証のレベルとを比較し、前記判定された認証のレベルが過去の認証のレベルと同等もしくはより低いレベルの場合は、前記受信側ユニットから前記要求された解読情報を送信することを特徴とするデジタルAVデータ送信方法。

【請求項25】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から1種類の認証ルールを選択する送信側認

証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルAVデータ送信ユニットであって、

認証の要求を行い、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段から1種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルAVデータ受信ユニットまたは、前記送信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルAVデータ送信ユニット。

【請求項26】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段から1種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルAVデータ送信ユニットに対して、認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記受信側複数認証ルール格納手段から1種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたデジタルAVデータ受信ユニットであって、前記送信ユニットまたは受信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルAVデータ受信ユニット。

【請求項27】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から1種類の認証ルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、前記受信側複数認証ルール格納手段から1種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルAVデータ受信ユニットとを備え、前記送信ユニットまたは受信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、前記重要度の判定を行ったユニットが重要度の判定を行わないユニットに前記選択した認証ルールについての情報

を送り、前記重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択することを特徴とするデジタルAVデータ送受信システム。

【請求項28】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証の要求を行い、デジタルAVデータの重要度を判定してその判定結果に基づいて、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段から1種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルAVデータ受信ユニットで選択される前記認証ルールと同じルールを、前記送信側複数認証ルール格納手段から選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ送信ユニット。

【請求項29】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段から受信側で選択される所定の認証ルールと同じ認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルAVデータ送信ユニットに対して、認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、そのデータ重要性判定手段の判定結果に基づいて、前記受信側複数認証ルール格納手段から1種類の認証ルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたことを特徴とするデジタルAVデータ受信ユニット。

【請求項30】 複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から受信側で選択される所定の認証ルールと同じルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、前記認証の要求を行う認証要求手段と、前記送信側複数認証ルール格納手段と同じ前記複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、そのデータ重要性判定手段の判定結果に基づいて、前記受信側複数認証ルール格納手段から1種類のルールを選択する受信側認証選択手段と、その選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルAVデータ受信ユニットとを備えたことを特徴とするデジタルAVデータ送受信システム。

【請求項31】 複数種類の認証ルールから1種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、前記受信ユニットからの認証要求を受け、前記格納されている管理基準を参照することにより認証するか否

かを判定する認証判定手段とを備えたデジタルAVデータ送信ユニットであって、前記認証要求を行う受信ユニットが、前記管理基準を持てない重要度の低い認証ルールのみで認証する機能しか有しない場合に、前記受信ユニットは、外部の管理センターからその受信ユニットに対応する前記管理基準用の識別情報が付与されるものであり、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルAVデータ送信ユニット。

【請求項32】 受信ユニットからの認証要求を受け、管理基準格納手段に格納されている受信ユニットに対する所定の管理基準を参照することにより認証するか否かを判定する認証判定手段を有するデジタルAVデータ送信ユニットに対し、前記認証要求を行う認証要求手段と、前記管理基準を持てない重要度の低い認証ルールのみで認証する認証手段とを備え、外部の管理センターから受信ユニット自身に対応する前記管理基準用の識別情報が付与されるデジタルAVデータ受信ユニットであって、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルAVデータ受信ユニット。

【請求項33】 複数種類の認証ルールから1種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、前記受信ユニットからの認証要求を受け、前記格納されている管理基準を参照することにより認証するか否かを判定する認証判定手段とを有するデジタルAVデータ送信ユニットと、その送信ユニットに対し、前記認証要求を行う認証要求手段と、前記管理基準を持てない重要度の低い認証ルールのみで認証する認証手段とを有し、外部の管理センターから受信ユニット自身に対応する前記管理基準用の識別情報が付与されるデジタルAVデータ受信ユニットとを備え、前記送信ユニットの認証判定手段は、前記認証要求の際に前記識別情報を受け取り、その識別情報が不可となった場合に、前記認証を取りやめることを特徴とするデジタルAVデータ送受信システム。

【請求項34】 前記所定の管理基準は、不正な、あるいは正当なデジタルAVデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のIDおよびそのIDに対する署名であることを特徴とする請求項31記載のデジタルAVデータ送信ユニット。

【請求項35】 前記認証判定手段は、前記ID及び署名の少なくとも一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項34記載のデジタルAVデータ送信ユニット。

【請求項36】 前記署名は、受信ユニットそれぞれに

あらかじめ固有に付加されている識別IDを利用して作成されるものであることを特徴とする請求項34、または35記載のデジタルAVデータ送信ユニット。

【請求項37】 前記所定の管理基準は、不正な、あるいは正当なデジタルAVデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のIDおよびそのIDに対する署名であることを特徴とする請求項32記載のデジタルAVデータ受信ユニット。

10 【請求項38】 前記認証判定手段は、前記ID及び署名の少なくとも一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項37記載のデジタルAVデータ受信ユニット。

【請求項39】 前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別IDを利用して作成されるものであることを特徴とする請求項37、または38記載のデジタルAVデータ受信ユニット。

20 【請求項40】 前記所定の管理基準は、不正な、あるいは正当なデジタルAVデータ受信ユニットを識別できる基準リストであり、前記識別情報が、前記受信ユニットに対応する前記管理基準用のIDおよびそのIDに対する署名であることを特徴とする請求項33記載のデジタルAVデータ送受信システム。

【請求項41】 前記認証判定手段は、前記ID及び署名の少なくとも一方が不可となった場合に、前記認証を取りやめることを特徴とする請求項40記載のデジタルAVデータ送受信システム。

30 【請求項42】 前記署名は、受信ユニットそれぞれにあらかじめ固有に付加されている識別IDを利用して作成されるものであることを特徴とする請求項40、または41記載のデジタルAVデータ送受信システム。

【請求項43】 請求項1～42のいずれかに記載のユニット又はシステムもしくは送信方法が有する各構成要素もしくはステップが持つ機能の全部又は一部を実現するためのプログラムを格納したことを特徴とする媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、AV装置間において認証を行う機能を持つAVシステムに関するものである。

【0002】

【従来の技術】従来のAV装置間において認証を行うシステムについて図2と図3を用いて説明する。

【0003】まず、図2において、デジタルAVデータ送信ユニットSTB18は、公開鍵と秘密鍵20、認証手段19、デジタルインターフェースD-I/F22、暗号化手段19を備えている。その公開鍵と秘密鍵20は、認証手段19を介して、デジタルインターフェースD-I/F22に接続している。また、暗号化手段19は、公開鍵と秘密鍵20を参照することが出来、デジタ

ルインターフェース22に接続している。デジタルAVデータ受信ユニットTV23も公開鍵と秘密鍵26、認証手段25、デジタルインターフェースD-I/F24、復号化手段27を具備している。その公開鍵と秘密鍵26は認証手段25を介してデジタルインターフェースD-I/F24に接続している。また、復号化手段27は公開鍵と秘密鍵26を参照することが出来、デジタルインターフェースD-I/F24に接続している。さらにデジタルインターフェースD-I/F22とデジタルインターフェースD-I/F24は互いにデータのやり取りが出来る構成となっている。

【0004】次にデジタルAVデータ送信ユニットSTB18とデジタルAVデータ受信ユニットTV23間の動作を説明する。まず、デジタルAVデータ受信ユニットTV23が認証要求を出す。するとデジタルインターフェースD-I/F24を通してデジタルAVデータ送信ユニットSTB18を構成するデジタルインターフェースD-I/F22に認証要求が到達する。デジタルインターフェースD-I/F22は認証要求を受けて認証手段19にて、公開鍵と秘密鍵20を参照して認証する。デジタルAVデータ送信ユニットSTB18にて認証されれば、暗号化手段21において、データが暗号化されて、デジタルインターフェースD-I/F22を介して、暗号化したデータが送信される。これはデジタルインターフェースD-I/F24を介して、公開鍵と秘密鍵26を参照して、復号化手段27で復号される。

【0005】このようにすると、偽造や改竄に強い機能が実現出来る。しかし、公開鍵と秘密鍵を用いた認証は多くの時間を要する。ニュースのように、あまり重要でないデータの場合、不必要に認証に時間を取られることがある。またVTRのようにコピー可能なデータしか受け取っては機器は、場合によってデジタルAVデータ受信ユニットが厳密な認証を要しないこともあり、そのような場合、時間の無駄が生じる。

【0006】次に、図3において、デジタルAV送信ユニットSTB28は共通鍵30、認証手段29、デジタルインターフェースD-I/F32、暗号化手段31を具備している。その共通鍵30は、認証手段29を介して、デジタルインターフェースD-I/F32に接続している。また、暗号化手段31は、共通鍵30を参照することが出来、デジタルインターフェース32に接続している。デジタルAVデータ受信ユニットTV33も、共通鍵36、認証手段35、デジタルインターフェース34、復号化手段37を具備している。その共通鍵36は認証手段35を介してデジタルインターフェース34に接続している。また、復号化手段37は共通鍵36を参照することが出来、デジタルインターフェース34に接続している。さらにデジタルインターフェース32とデジタルインターフェース34は互いにデータのやり取りが出来る構成となっている。

【0007】次にデジタルAVデータ送信ユニットSTB28とデジタルAVデータ受信ユニットTV33間の動作を説明する。まず、デジタルAV受信ユニットTV33が認証要求を出す。するとデジタルインターフェースD-I/F34を通してデジタルAV送信ユニットSTB28を構成するデジタルインターフェースD-I/F32に認証要求が到達する。デジタルインターフェースD-I/F32は認証要求を受けて認証手段29にて、共通鍵30を参照して認証する。デジタルAV送信ユニットSTB28にて認証されれば、暗号化手段31において、データが暗号化されて、デジタルインターフェースD-I/F32を介して、暗号化したデータが送信される。これはデジタルインターフェースD-I/F34を介して、共通鍵36を参照してデジタル復号化手段37で復号される。

【0008】このようにすると、短い時間でデータの認証を行うことができる。しかし、共通鍵を用いた認証は偽造や改竄に弱いので、新作の映画など著作権上重要なデータの場合、第三者にデータを無料で視聴されることがある。またTVのように受信した全てのデータを表示するために、厳密な認証を行う機器と接続した場合に対応できる必要があり、デジタルAVデータ受信ユニットが厳密な認証を要する場合があります、そのような場合重要なデータの著作権が保護されないといったことが起こりうる。

【0009】

【発明が解決しようとする課題】このように、あまり重要でないデータの認証に多くの時間を要するという課題や、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題が存在する。また、デジタルAVデータ受信ユニットによっては、厳密な認証を要しないものも存在し、このようなユニットに対して厳密な認証を行った場合、時間の無駄が生じるという課題や、逆にデジタルAVデータ受信ユニットによっては厳密な認証を要するものも存在し、そのようなユニットに厳密でない認証を行った場合、著作権が守られないといった課題が存在する。更に、不正使用の防止のために、厳密な認証と厳密でない認証とで、暗号鍵を各々に対応して用意した場合、厳密な認証を行って暗号鍵を取得した後

に、厳密でないデータを必要とする場合でも、改めて厳密でない認証を行う必要がある。また、受信側が機器の排除機能を持たない機器の場合は、送信側は不正な機器を排除できない構成になっているという課題がある。

【0010】本発明は、このような従来の、重要でないデータの認証に多くの時間を要するという課題と、重要なデータであるにもかかわらずその認証が偽造や改竄に弱いという課題と、ユニットによって認証に必要な厳密さが異なるといった課題を考慮し、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法でデータの送受信を行いうるユニット、シ

システム等を提供することを目的とするものである。

【0011】

【課題を解決するための手段】上述した課題を解決するために、請求項1の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルAVデータ送信ユニットである。

【0012】また請求項2の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAVデータ送信ユニットを通信の対象とし、認証の要求を行う認証要求手段と、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも備えたデジタルAVデータ受信ユニットである。

【0013】また請求項3の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類のルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、認証の要求を行う認証要求手段と、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有するデジタルAVデータ受信ユニットとを備えたデジタルAVデータ送受信システムである。

【0014】また請求項4の本発明は、デジタルAVデータの重要度を判定するデータ重要性判定手段と、所定の管理基準を格納した管理基準格納手段と、認証要求を受け、データ重要性判定手段の判定結果に基づき、管理基準格納手段の管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って管

理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたデジタルAVデータ送受信システムである。

【0015】また請求項5の本発明は、送信ユニットは受信ユニットの各機能を有し、受信ユニットは送信ユニットの各機能を有する請求項3記載のデジタルAVデータ送受信システムである。

10 【0016】また請求項6の本発明は、受信ユニットの機能を有する送信ユニット、あるいは送信ユニットの機能を有する受信ユニットが三つ以上互いに接続され、デジタルAVデータを互いにやりとりできる請求項5記載のデジタルAVデータ送受信システムである。

20 【0017】また請求項7の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルAVデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも備えたデジタルAV送信ユニットである。

また請求項8の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルAVデータ受信ユ

30 ニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットを通信の対象とし、認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、送信ユニットとの間で認証ルールにて認証を行う受信側認証手段とを少なくとも備えたデジタルAVデータ受信ユニットである。

40

【0018】また請求項9の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、デジタルAVデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証ルール取り出し手段と、それに基づき認証を行う送信側認証手段とを少なくとも有するデジタルAV送信ユニットと、認証

50

の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、送信ユニットとの間で認証ルールにて認証を行う受信側認証手段を少なくとも有するデジタルAVデータ受信ユニットとを備えたデジタルAVデータ送受信システムである。

【0019】また請求項10の本発明は、所定の管理基準を格納した管理基準格納手段と、デジタルAVデータ受信ユニットから認証要求を受けて、そのデジタルAVデータ受信ユニットの種類又は重要度に応じて、管理基準格納手段の管理基準を参照すべきかどうか決定する管理基準参照決定手段と、その決定された結果に従って管理基準を参照してそれに従い認証すべきかどうか、あるいは認証の種類を決定する認証決定手段と、その認証決定手段の決定に従って、所定の認証ルールに基づいて認証を行う認証手段とを少なくとも備えたデジタルAV送信ユニットである。

【0020】また請求項11の本発明は、管理基準は、不正な、あるいは正当なデジタルAVデータ受信ユニットを識別できる基準リスト(CRL)である請求項4又は10に記載のデジタルAV送信ユニットである。

【0021】また請求項12の本発明は、送信ユニットに、受信ユニットが二つ以上接続され、送信ユニットとの間で、デジタルAVデータをやりとりできる請求項9記載のデジタルAVデータ送受信システムである。

【0022】また請求項13の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、単一認証デジタルAVデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、送信側認証選択手段又は送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも備えたデジタルAVデータ送信ユニットである。

【0023】また請求項14の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、デジタルAVデータの重要度を判定するデータ重要性判定手段と、データ重要性判定手段の判定結果に基づき、送信側複数認証ルール格納手段から一種類の認証ルールを選択する送信側認証選択手段と、単一認証デジタルAVデータ受信ユニットが有する一種類の認証ルールについての情報を受け取るユニット認証ルール情報受信手段

と、ユニット認証ルール情報受信手段で受信された認証ルールについての情報に基づき、単一認証デジタルAVデータ受信ユニットが有する認証ルールを、送信側複数認証ルール格納手段から取り出す送信側認証取り出し手段と、送信側認証選択手段又は送信側認証取り出し手段から得られた認証ルールに基づき認証を行う送信側認証手段とを少なくとも有するデジタルAVデータ送信ユニットと、認証の要求を行う認証要求手段と、送信側認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段と、送信側認証選択手段で選択された所定の認証ルールと同じ認証ルールを受信側複数認証ルール格納手段から選択する受信側認証選択手段と、受信側で選択された認証ルールに基づいて認証を行う受信側認証手段とを少なくとも有する複数認証デジタルAVデータ受信ユニットと、認証の要求を行う認証要求手段と、自らの一種類の認証ルールを格納する受信側単一認証ルール格納手段と、認証ルールについての情報を送信する認証ルール情報送信手段と、デジタルAVデータ送信ユニットとの間で認証ルールにて認証を行う受信側認証手段を少なくとも有する単一認証デジタルAVデータ受信ユニットとを備えたデジタルAVデータ送受信システムである。

【0024】また請求項15の本発明は、複数認証デジタルAVデータ受信ユニットはデジタルAVデータ送信ユニットの各機能を有し、デジタルAVデータ送信ユニットは複数認証デジタルAVデータ受信ユニットの各機能を有する請求項14記載のデジタルAVデータ送受信システムである。

【0025】また請求項16の本発明は、複数認証デジタルAVデータ受信ユニットの各機能を有するデジタルAVデータ送信ユニット、あるいはデジタルAVデータ送信ユニットの機能を有する複数認証デジタルAVデータ受信ユニットが二つ以上互いに接続され、且つ、単一認証デジタルAVデータ受信ユニットが二つ以上接続され、デジタルAVデータを互いにやりとりできる請求項15記載のデジタルAVデータ送受信システムである。

【0026】請求項17の本発明は、デジタルAVデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルAVデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルAVデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、受信ユニットに送信する解読情報選択手段とを備えた送信ユニットである。

【0027】請求項18の本発明は、データの重要度に応じた複数のレベルで暗号化されたデジタルAVデータを送信する送信ユニットから受信した暗号化されたデー

10

20

30

40

50

タを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等及びそれ以下のレベルの暗号化データに対する解読情報の全部、又は一部を、送信ユニットに要求する解読情報要求手段とを備えた受信ユニットである。

【0028】請求項19の本発明は、デジタルAVデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルAVデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルAVデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、受信ユニットに送信する解読情報選択手段とを有する送信ユニットと、その送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等及びそれ以下のレベルの解読情報の全部、又は一部を、送信ユニットに要求する解読情報要求手段とを有する受信ユニットとを備えたデジタルAVデータ送受信システムである。

【0029】請求項20の本発明は、デジタルAVデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルAVデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルAVデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等のレベルの解読情報を受信ユニットに送信する解読情報選択手段とを備え、解読情報選択手段は、次に受信ユニットから解読情報の要求があった時に、その要求が判定済みの認証レベルと同等あるいはそれ以下のレベルの解読情報の場合は、認証手続きを省略して要求された解読情報を受信ユニットに送信する送信ユニットである。

【0030】請求項21の本発明は、データの重要度に応じた複数のレベルで暗号化されたデジタルAVデータを送信する送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等のレベルの暗号化データに対する解読情報を送信ユニットに要求する解読情報要求手段とを備え、解読情報要求手段は、認証のレベルと同等あ

るいはそれ以下のレベルの解読情報を送信ユニットに要求する時は、認証要求を行わずに、解読情報の要求を行う受信ユニットである。

【0031】請求項22の本発明は、デジタルAVデータを、そのデータの重要度に応じた複数のレベルで暗号化する暗号化手段と、暗号化されたデジタルAVデータを受信する受信ユニットから要求された認証レベルの認証を行う認証手段と、その認証手段により認証された認証レベルを判定するレベル判定手段と、認証の後、受信ユニットからの、暗号化されたデジタルAVデータを解読するための解読情報の要求に対して、判定済みの認証レベルと同等のレベルの解読情報を受信ユニットに送信する解読情報選択手段とを有し、解読情報選択手段は、次に受信ユニットから解読情報の要求があった時に、その要求が判定済みの認証レベルと同等あるいはそれ以下のレベルの解読情報の場合は、認証手続きを省略して要求された解読情報を受信ユニットに送信する送信ユニットと、その送信ユニットから受信した暗号化されたデータを解読するために必要な認証レベルを決定するレベル決定手段と、その決定された認証レベルの認証を送信ユニットに要求する認証手段と、送信ユニットによる認証の後、認証レベルと同等のレベルの解読情報を送信ユニットに要求する解読情報要求手段とを備え、解読情報要求手段は、認証のレベルと同等あるいはそれ以下のレベルの解読情報を送信ユニットに要求する時は、認証要求を行わずに、解読情報の要求を行うとを有する受信ユニットとを備えたデジタルAVデータ送受信システムである。

【0032】請求項25の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、その送信側複数認証ルール格納手段から1種類の認証ルールを選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルAVデータ送信ユニットであって、認証の要求を行い、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認証ルール格納手段から1種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルAVデータ受信ユニットまたは、送信ユニットにおける認証ルールの選択は、データの重要度の判定結果に基づいて行われ、重要度の判定を行ったユニットが重要度の判定を行わないユニットに選択した認証ルールについての情報を送り、重要度の判定を行わないユニットは、その情報に基づいて、同じ認証ルールを選択するデジタルAVデータ送信ユニットである。

【0033】請求項28の本発明は、複数種類の認証ルールを格納した送信側複数認証ルール格納手段と、認証の要求を行い、デジタルAVデータの重要度を判定してその判定結果に基づいて、送信側複数認証ルール格納手段と同じ複数種類の認証ルールを格納した受信側複数認

証ルール格納手段から一種類の認証ルールを選択し、その選択された認証ルールに基づいて認証を行うデジタルAVデータ受信ユニットで選択される認証ルールと同じルールを、送信側複数認証ルール格納手段から選択する送信側認証選択手段と、その選択された認証ルールに基づいて認証を行う送信側認証手段とを少なくとも備えたデジタルAVデータ送信ユニットである。

【0034】請求項31の本発明は、複数種類の認証ルールから1種類の認証ルールを選択して認証を行う認証手段と、受信ユニットに対する所定の管理基準を格納した管理基準格納手段と、受信ユニットからの認証要求を受け、格納されている管理基準を参照することにより認証するか否かを判定する認証判定手段とを備えたデジタルAVデータ送信ユニットであって、認証要求を行う受信ユニットが、管理基準を持ってない重要度の低い認証ルールのみで認証する機能しか有しない場合に、受信ユニットは、外部の管理センターからその受信ユニットに対応する管理基準用の識別情報が付与されるものであり、送信ユニットの認証判定手段は、認証要求の際に識別情報を受け取り、その識別情報が不可となった場合に、認証を取りやめるデジタルAVデータ送信ユニットである。

【0035】請求項43の本発明は、請求項1～42のいずれかに記載のユニット又はシステムもしくは送信方法が有する各構成要素もしくはステップが持つ機能の全部又は一部を実現するためのプログラムを格納した媒体である。

【0036】

【発明の実施の形態】以下に本発明の実施の形態を図面を参照して説明する。

【0037】まず、第一の実施の形態について図1を参照して説明する。

【0038】デジタルAVデータ送信ユニットSTB1は、データ重要性判定手段3、暗号化手段4、送信側複数認証ルール格納手段5、送信側認証選択手段6、送信側認証手段7及びデジタルインターフェースD-I/F8を持つ。このデータ重要性判定手段3は、データ2の重要性を重要度に応じて複数種類に場合分けを行う手段である。このデータの重要度はCGMSで表現されている。このCGMSは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段4は、データ2を、認証の過程で作成されたワーク鍵Kcol6で暗号化する手段である。ワーク鍵Kcol6を生成するその認証方法は後述する。送信側複数認証ルール格納手段5は、複数種類の認証ルールを持つ手段である。例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールの2種類の認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段6は、送信側複数認証ルール格納手

段5が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この際、データ重要性判定手段3の判定の結果を参考にする。本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、時間はかからないが、偽造や改竄に弱いルールとして、共通鍵を用いた認証ルールを選択する。送信側認証手段7は、選択された認証ルールで実際にデジタルAVデータ受信ユニットTV9と認証をかわす手段である。デジタルインターフェースD-I/F8は、デジタルAVデータ受信ユニットTV9とAVデータや信号のやりとりを行う手段である。

【0039】デジタルAVデータ受信ユニットTV9は、デジタルインターフェースD-I/F10、復号化手段11、認証要求手段12、受信側認証手段13、受信側複数認証ルール格納手段14、受信側認証選択手段15を持つ。この認証要求手段12は、デジタルAVデータ送信ユニットSTB1に認証要求を出す手段である。また、受信側複数認証ルール格納手段14は、送信側複数認証ルール格納手段5に格納された複数の認証ルールと同じ複数の種類の認証ルールを持つ手段である。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールを持つ。受信側認証選択手段15は上述した受信側複数認証ルール格納手段14から、送信側認証選択手段6で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段13は、その選択された認証ルールで、つまりデジタルAVデータ送信ユニットSTB1で選択された認証ルールを用いて実際にデジタルAVデータ送信ユニットSTB1と認証を互いに交わす手段である。復号化手段11はデジタルAVデータ送信ユニットSTB1で暗号化され送信されてきたデジタルAVデータをワーク鍵Kcol7を用いて復号化する手段である。ワーク鍵Kcol7は前記受信側認証過程で生成されるもので、その生成する方法は前記ワーク鍵Kcol6を生成する方法とともに後述する。デジタルインターフェースD-I/F10は、送信ユニットSTB1とAVデータや信号のやりとりを行う手段である。

【0040】次に、このような本実施の形態の動作を説明する。

【0041】まず、デジタルAVデータ受信ユニットTV9を構成する、認証要求手段12が、デジタルインターフェースD-I/F10を介して、デジタルAVデータ送信ユニットSTB1に自らのIDを含めて認証要求を出す。もちろんAVデータの送信要求も出す。デジタルAVデータ送信ユニットSTB1は、デジタルインターフェースD-I/F8を介して、前記認証要求を受信する。そうするとデジタルAVデータ送信ユニットSTB1は、まずデータ重要性判定手段3で、これから送信すべきAVデータ2の重要性を判定し場合分けする。す

なわちCGMSの値が11なら重要度は高く、そのデータは表示のみ可能であり、コピーすることは禁止される。また、CGMSの値が10の場合は一回のみコピー可能であり、比較的重要なデータである。またCGMSが00の場合は自由に視聴ないしはコピーして使用してよいので、重要でないデータと言える。またCGMSが01となるAVデータは存在しない。このCGMSの値によりデータの重要度の場合分けがなされる。この結果は送信側認証選択手段6に送られ、送信側複数認証ルール格納手段5から最適な認証ルールが選択される。すなわち、最新の映画など重要なデータの場合には、時間がかかるが、偽造や改竄に強い、公開鍵と秘密鍵を用いる認証ルールが選択される。また、ニュースのような重要でないデータの場合には、時間はかからないが、偽造や改竄に弱い、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段7に送られ、デジタルインターフェースD-I/F8を介して、デジタルAV受信ユニットTV9に送られる。デジタルAV受信ユニットTV9においては、受信側認証選択手段15が、その選択情報を利用して受信側複数認証ルール格納手段14から、デジタルAVデータ送信ユニットSTB1で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。そこで、受信側認証手段13と送信側認証手段7とは互いに、デジタルインターフェースD-I/F10およびデジタルインターフェースD-I/F8を介して、認証を行う。認証が成功すれば、後述するようにして送信側にワーク鍵Kcol6、また受信側にワーク鍵Kcol7が生成される。送信すべきデータ2は生成されたワーク鍵Kcol6を用いて、暗号化手段4で暗号化される。そのあと、デジタルインターフェースD-I/F8を介して、デジタルAVデータ受信ユニットTV9に暗号化データとして送信される。デジタルインターフェースD-I/F10を介して暗号化されたデータは、ワーク鍵Kcol7を用いて、復号化手段11にて復号化され、データ101になる。これはデータ2と同一のデータであり、デジタルAVデータ送信ユニットSTB1から、デジタルAVデータ受信ユニットTV9にデータが送信されたことになる。

【0042】最後に、デジタルAVデータ受信ユニットTV9は、ディスプレイ装置の画面にそのデータを表示する。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証手段が用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【0043】次に前述したようにデジタルAVデータ受信ユニットTV9からデジタル送信ユニットSTB1に認証要求が出たときの認証のやりとりを示し、その結果ワーク鍵Kcoを生成する実施の形態を図4と図5を参照して説明する。

【0044】まず、図4に示すとき、公開鍵と秘密鍵による認証を行う場合である。この場合受信側は秘密鍵Sbと公開鍵Paを持つ。また送信側は秘密鍵Saと公開鍵Paを持つ。まずステップ1で受信側が乱数Bを発生する。受信側は自己の認識番号であるIDbと乱数Bを自らの秘密鍵Sbで暗号化した暗号文Sb(B)を送信側に送る。送信側は受信側の認識番号IDbから検索して受信側の公開鍵Pbを入手する。ステップ8で入手した公開鍵Pbで暗号文Sb(B)を復号化する。その結果ステップ9のごとく乱数Bが得られる。さらに、送信側は、ステップ10のごとく乱数Aを発生する。乱数AとBは送信側の秘密鍵Saで暗号化され暗号文Sa(A, B)が作成される。送信側は暗号文Sa(A, B)と自己の認識番号IDaを受信側に送信する。受信側は暗号文Sa(A, B)と送信側の認識番号IDaを受け取る。受信側は、送信側の認識番号IDaから検索して送信側の公開鍵Paを入手し、ステップ2のごとく、Paで暗号文Sa(A, B)を復号化する。ここで、暗号文Sa(A, B)から受信側にはステップ1で送った乱数Bと全く同一の乱数Bが得られ、偽造や改竄が行われていないことが受信側にわかる。もし前記2つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵Pa, Pbは正当な者にしか入手できないようになっているものとする。次に受信側はステップ3のごとく、受信側の秘密鍵Sbで乱数Aを暗号化し、暗号文Sb(A)を作成する。Sb(A)は送信側に送られ、ステップ11のごとく既に送信側で持っている、受信側の公開鍵Pbで暗号文Sb(A)を復号化する。ステップ10で発生した、乱数Bとステップ11で復号化した乱数Bは全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記2つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【0045】今、受信側と送信側でやりとりした乱数AとBは偽造や改竄が行われていないとすると、受信側と送信側以外の第3者には乱数AとBは秘密の乱数である。そこで送信側で、ステップ12のごとく、乱数AとBを用いて鍵Kabを作成する。同じくステップ4のごとく受信側で乱数AとBを用いて鍵Kabを作成する。前記2つのKabは全く同一のものであり共通鍵となっている。次に送信側でステップ13のごとく鍵Kexを作成する。これを共通鍵Kabで暗号化し、暗号文Kab(Kex)を作成して、受信側に送る。受信側はステップ5のごとく共通鍵Kabで暗号文Kab(Kex)を復号化してKexを得、その結果、受信側が得た鍵Kexと送信側にある鍵Kexは全く同一であり、共通鍵となる。次に送信側でステップ14のごとく鍵Kcoを作成する。鍵Kcoは共通鍵Kexで暗号化され、暗号文Kex(Kco)として、受信側に送られる。受信側では、ステップ6のごと

く共通鍵 K_{ex} で暗号文 K_{ex} (K_{co}) を復号化し、ステップ7のごとく K_{co} を得る。送信側にある鍵 K_{co} と受信側にある K_{co} は全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵 K_{co} である。

【0046】次に図5に示すとき、共通鍵による認証を行う場合の説明をする。この場合、送信側と受信側は共通鍵 S を持つ。なお、この共通鍵は正当な者にしか与えられていない。まず、受信側でステップ15のごとく2個の乱数 A_1 、 A_2 を発生し、共通鍵 S で暗号化し、暗号文 $S(A_1A_2)$ を作成し、送信側へ送る。送信側ではステップ20のごとく共通鍵 S で暗号文 $S(A_1A_2)$ を復号化する。そうすると、ステップ21のごとく乱数 A_1 と乱数 A_2 が得られる。送信側は乱数 A_2 を受信側に送る。受信側はステップ16のごとく2つの乱数 A_1 と A_2 を持つことになる。ステップ15で発生した乱数 A_2 とステップ16で送信側から受け取った乱数 A_2 が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記2つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ22のごとく乱数 B_1 と B_2 を発生し、暗号化して、暗号文 $S(B_1B_2)$ を受信側に送る。受信側はステップ17のごとく共通鍵 S を用いて暗号文 $S(B_1B_2)$ を復号化する。すると、ステップ18のごとく乱数 B_1 と B_2 が得られる。受信側は乱数 B_2 を送信側に送る。送信側はステップ23のごとく乱数 B_1 と B_2 を持つことになる。ステップ22で発生した乱数と、ステップ23で受信側から受け取った乱数 B_2 が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記2つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【0047】ここまでで、認証が成功しているとする。と、乱数 A_1 と乱数 B_1 は送信側と受信側以外の第3者には秘密の乱数である。送信側ではステップ24のごとく乱数 A_1 と乱数 B_1 から鍵 K_{co} を作成する。一方受信側では、ステップ19のごとく乱数 A_1 と乱数 B_1 から鍵 K_{co} を作成する。送信側にある鍵 K_{co} と受信側にある鍵 K_{co} は全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵 K_{co} である。

【0048】なお、本発明において、選択する認証ルールの種類は、前記公開鍵及び秘密鍵と共通鍵との2種類に限らず、その他の種類でもよく、更に3種類以上の異なる認証ルールを使用するものであってもよい。

【0049】また、本実施の形態の変形例として、デジタルAVデータ送信ユニット1はデジタルAV受信ユニット9と同じ機能を有し、また、デジタルAVデータ受信ユニット9はデジタルAV送信ユニット1と同じ機能を有するようになっていてもよい。以後それらのユニット

のことを、デジタルAVデータ送受信ユニットと呼ぶ。またそれらの送受信ユニットが3台以上が互いに接続されていてよい。

【0050】次に本発明の第二の実施の形態について図6を参照して説明する。

【0051】本実施の形態では、第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対して、デジタルAVデータ受信ユニットVTR45が有する認証ルールの種類によって、認証ルールを選択するところが、相違点である。

【0052】デジタルAVデータ送信ユニットSTB38は、送信側複数認証ルール格納手段41等を持つ。送信側複数認証ルール格納手段41は、複数種類の認証ルールを持つ手段である。これは第一の実施の形態で説明したごとく、例えば、公開鍵と秘密鍵を用いた認証ルールと、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。ユニット認証ルール情報受信手段42は、デジタルAVデータ受信ユニットVTR45から送られて来た認証ルールに関連する情報を受信する手段である。送信側認証取り出し手段53は、その認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段41から所定の認証ルールを取り出し、送信側認証手段43に渡す手段である。送信側認証手段43は、デジタルAV受信ユニットVTR45と互いに認証を交わす手段である。暗号化手段40は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵 K_{co} 53により、データ39を暗号化する手段である。デジタルインターフェースD-U/F44は、デジタルAVデータ受信ユニットVTR45とデータや信号のやりとりをする手段である。

【0053】デジタルAVデータ受信ユニットVTR45は、受信側認証ルール格納手段49等を持つ。この受信側認証ルール格納手段49は、第一の実施の形態で説明した場合とは違って、一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段49に格納されている認証ルールはデジタルAVデータ受信ユニットVTR45の装置の性質あるいは重要度によって、あらかじめ決められている。すなわちデータの再利用を予定しないTVなどのユニットには時間はかかるが、偽造や改竄に強い認証ルールが格納されており、またデータのコピーを前提とするVTRのようなユニットには、時間はかからないが、偽造や改竄に弱い認証ルールが格納されている。これによって、AVデータの著作権を守ることができる。本実施の形態では デジタルAVデータ受信ユニットVTR45はVTRであるので、受信側認証ルール格納手段49は共通鍵を持つものとし

て説明をする。認証ルール情報送信手段50は、デジタルAVデータ受信ユニットVTR45が受信側認証ルール格納手段49に有する共通鍵による認証ルールに関連する情報を送信する手段である。受信側認証手段51は、デジタルAV送信ユニットSTB38と互いに認証を交わす手段である。復号化手段47は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Kco54により、暗号化されたデータを復号化する手段である。

【0054】次にこのような本実施の形態の動作を説明する。

【0055】まず、デジタルAVデータ受信ユニットVTR45を構成する、認証要求手段48がデジタルインターフェースD-I/F46を介して、デジタルAVデータ送信ユニットSTB38に認証要求を出す。デジタルAVデータ送信ユニットSTB38は、デジタルインターフェースD-I/F44を介して、前記認証要求を受信する。また同時に、認証ルール情報送信手段50が、受信側認証ルール格納手段49を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースD-I/F46を介して、デジタルAVデータ送信ユニットSTB38に送る。ユニット認証ルール情報受信手段42が、デジタルAVデータ受信ユニットVTR45から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースD-I/F44を介して、受け取る。さらに、この認証ルールの識別子は、送信側認証ルール取り出し手段55に渡され、送信側複数認証ルール格納手段41から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出す。その後、取り出された共通鍵による認証ルールは、送信側認証手段43に渡される。その後、送信側認証手段43と受信側認証手段51は互いに、デジタルインターフェースD-I/F44とD-I/F46を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で説明したごとく、送信側にワーク鍵Kco53、受信側にワーク鍵Kco54が生成される。データ39は暗号化手段40にてワーク鍵Kco53により暗号化される。暗号化されたデータはデジタルインターフェースD-I/F44を介して、デジタルAV受信ユニットVTR45に送られる。デジタルインターフェースD-I/F46を介して暗号化されたデータは、復号化手段47に送られ、ワーク鍵Kco54を用いて復号化され、データ52が得られる。

【0056】なお、本発明において、送信側の認証ルールの種類は、前記共通鍵に限らず、公開鍵及び秘密鍵、またその他の種類でもよく、更に3種類以上の異なる認証ルールを使用するものであってもよい。

【0057】また、デジタルAVデータ受信ユニットは

2台あり、その一つは共通鍵による認証ルールのみ有し、他の一つは公開鍵及び秘密鍵のみを有するものであってもよい。さらに3台以上のデジタルAVデータ受信ユニットであってもよい。

【0058】次に本発明の第三の実施の形態について図7を参照して説明する。

【0059】第一の実施の形態がデータの重要度に応じて認証ルールを変えていたのに対し、また、第二の実施の形態がデジタルAVデータ受信ユニットの種類によって認証ルールを変えていたのに対し、本実施の形態では、データの重要度とデジタルAV受信ユニットの種類の両方で認証ルールを決めるところが特徴である。

【0060】本実施の形態では、デジタルAVデータ送信ユニットSTB56と、複数認証デジタルAVデータ受信ユニットTV65と、単一認証デジタルAVデータ受信ユニットVTR72の三種類のユニットを扱う。デジタルAVデータ送信ユニットSTB56は複数認証デジタルAVデータ受信ユニットTV65と単一認証デジタルAVデータ受信ユニットVTR72にデータを送信するユニットである。複数認証デジタルAVデータ受信ユニットTV65に対しては、デジタルAVデータ送信ユニットSTB56においてデータの重要度により複数種類の認証ルールを選択して、そのデータを送信する。また、単一認証デジタルAVデータ受信ユニットVTR72は自らの持つ一つの認証ルールを用いてデジタルAVデータ送信ユニットSTB56とで認証を行うユニットである。

【0061】デジタルAVデータ送信ユニットSTB56は、データ重要性判定手段57を持つ。これは、データ82の重要性を重要度に応じて複数種類の場合分けを行う手段である。この重要度は第一の実施の形態で説明したごとくCGMSで表現されている。このCGMSは放送局から送られてくるデータの内部あるいはヘッダーに存在している。暗号化手段64は、データ82を認証の過程で作成されたワーク鍵Kco79で暗号化する手段である。ワーク鍵Kco79を生成する過程は第一の実施の形態で説明した。送信側複数認証ルール格納手段63は、複数種類の認証ルールを持つ。例えば、公開鍵と秘密鍵を用いた認証ルールや、共通鍵を用いた認証ルールである。ここでは、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールが格納されているとして説明を進める。送信側認証選択手段59は、送信側複数認証ルール格納手段63が持つ複数種類の認証ルールから一種類の認証ルールを選択する手段である。この時、データ重要性判定手段57の場合分けの結果を参考にする。第一の実施の形態のごとく、本実施の形態では、前記の重要度が高いか低いかにより、時間はかかるが偽造や改竄に強い認証ルールとして、公開鍵と秘密鍵を用いた認証ルールを選択し、また、時間はかからないが、偽造や改竄に弱い認証ルールとして、共通鍵を用いた認証

ルールを選択する。ユニット認証ルール情報受信手段60は、単一認証デジタルAVデータ受信ユニットVTR72から送られて来た認証ルールに関する情報を受信する手段である。送信側認証ルール取り出し手段58は、認証ルールに関連する情報に基づいて、送信側複数認証ルール格納手段63から所定の認証ルールを取り出し、送信側認証手段61に渡す手段である。送信側認証手段61は、実際に複数認証デジタルAVデータ受信ユニットTV65及び単一認証デジタルAVデータ受信ユニットVTR72と認証を交わす手段である。デジタルインターフェースD-I/F62は、複数認証デジタルAVデータ受信ユニットTV65や単一認証デジタルAVデータ受信ユニットVTR72とAVデータや信号をやりとりする手段である。

【0062】複数認証デジタルAVデータ受信ユニットTV65は、認証要求手段67を持つ。これは、デジタルAVデータ送信ユニットSTB56に認証要求を出す手段である。また、受信側複数認証ルール格納手段68は、送信側複数認証ルール格納手段63と同じ複数種類の認証ルールを持つ。従って本実施の形態の場合、公開鍵及び秘密鍵を用いた認証ルールと共通鍵を用いた認証ルールがある。受信側認証選択手段69は、受信側複数認証ルール格納手段68から、送信側認証選択手段59で選択された認証ルールと同じ認証ルールを選択する手段である。受信側認証手段70は、その選択された認証ルールで、つまりデジタルAVデータ送信ユニットSTB56で選択された認証ルールを用いて実際にデジタルAVデータ送信ユニットSTB56と認証を互いに交わす手段である。復号化手段66は、デジタルAVデータ送信ユニットSTB56で暗号化されたデジタルAVデータをワーク鍵Kco80を用いて復号化する手段である。ワーク鍵Kco80は前記認証過程で生成されるもので、その生成する方法は前記ワーク鍵Kco79とともに第一の実施の形態で説明した。デジタルインターフェースD-I/F71は、デジタルAVデータ送信ユニットSTB56とAVデータや信号のやりとりを行う手段である。

【0063】単一認証デジタルAVデータ受信ユニットVTR72は、受信側認証ルール格納手段75を持つ。これは、前述したごとく一種類の認証ルールのみ格納する手段である。例えば、公開鍵と秘密鍵を用いた認証ルール、あるいは共通鍵を用いた認証ルールのような認証ルールがある。ここで、受信側認証ルール格納手段75に格納されている認証ルールは単一認証デジタルAVデータ受信ユニットVTR72の装置の種類や、重要度によって、あらかじめ決められている。ここでは、受信側認証ルール格納手段75が共通鍵を持つものとして説明をする。認証ルール情報送信手段76は、単一認証デジタルAVデータ受信ユニットVTR72が受信側認証ルール格納手段75に有する共通鍵による認証ルールに関

連する情報を送信する手段である。受信側認証手段77は、デジタルAVデータ送信ユニットSTB56と互いに認証を交わす手段である。復号化手段73は、第一の実施の形態で説明したごとく、認証を交わした結果生成されたワーク鍵Kco81により、暗号化されたデータを復号化する手段である。

【0064】次にこのような本実施の形態の動作を説明する。まず、はじめに複数認証デジタルAVデータ受信ユニットTV65かまたは単一認証デジタルAVデータ受信ユニット72が認証要求を出す。デジタルAVデータ送信ユニットSTB56はどのユニットから認証要求が送られて来たのかを判断する。

【0065】以下、まず複数認証デジタルAVデータ受信ユニットTV65から認証要求が来た場合を説明し、次に単一認証デジタルAVデータ受信ユニットVTR72から認証要求が来た場合の説明を行う。

【0066】第一に、前述したように複数認証デジタルAVデータ受信ユニットTV65を構成する、認証要求手段67が、デジタルインターフェースD-I/F71を介して、デジタルAVデータ送信ユニットSTB56に自らのIDを含めて認証要求を出す。デジタルAVデータ送信ユニットSTB56は、デジタルインターフェースD-I/F62を介して、前記認証要求を受信する。そうするとデジタルAVデータ送信ユニットSTB56は、まずデータ重要性判定手段57で、これから送信すべきデータ82の重要性を判定し場合分けする。この結果は送信側認証選択手段59に送られ、送信側複数認証ルール格納手段63から最適な認証ルールが選択される。すなわち、重要なデータの場合には、公開鍵と秘密鍵を用いる認証ルールが選択される。また、重要でないデータの場合には、共通鍵を用いる認証ルールが選択される。更にその選択情報は、送信側認証手段61に送られ、デジタルインターフェースD-I/F62を介して、複数認証デジタルAVデータ受信ユニットTV65に送られる。複数認証デジタルAVデータ受信ユニットTV65においては、受信側認証選択手段69が、その選択情報を利用して受信側複数認証ルール格納手段68からデジタルAVデータ送信ユニットSTB56で選択された認証ルールと同じ認証ルールを選択する。従って選択されている認証ルールは送信側と受信側とで同じになる。受信側認証手段70と送信側認証手段61とは互いに、デジタルインターフェースD-I/F71およびデジタルインターフェースD-I/F62を介して、認証を行う。認証が成功すれば、第一の実施の形態で詳述したごとく、送信側にワーク鍵Kco79、また受信側にワーク鍵Kco80が生成される。送信すべきデータ82は生成されたワーク鍵Kco79を用いて、暗号化手段64で暗号化される。そのあと、デジタルインターフェースD-I/F62を介して、複数認証デジタルAVデータ受信ユニットTV65に暗号化されたデータとして送

信される。デジタルインターフェースD-I/F71を介して暗号化されたデータは、ワーク鍵Kco80を用いて、復号化手段66にて復号化され、データ83になる。これはデータ82と同一のデータであり、デジタルAVデータ送信ユニットSTB56から、複数認証デジタルAVデータ受信ユニットTV65にデータが送信されたことになる。このようにして、データの重要性が高い時は、時間はかかるが、偽造や改竄に強い認証ルールが用いられ、またデータの重要性が低い時は、時間はかからないが、偽造や改竄に弱い認証ルールが用いられる。

【0067】次に単一認証デジタルAVデータ受信ユニットVTR72から認証要求が来た場合の動作の説明を行う。まず、単一認証デジタルAVデータ受信ユニットVTR72を構成する、認証要求手段74がデジタルインターフェースD-I/F78を介して、デジタルAVデータ送信ユニットSTB56に認証要求を出す。デジタルAVデータ送信ユニットSTB56は、デジタルインターフェースD-I/F62を介して、前記認証要求を受信する。同時に認証ルール情報送信手段76が、受信側認証ルール格納手段75を参照し、格納されている認証ルール、つまり共通鍵による認証ルールに関する情報を取り出す。例えば、その共通鍵による認証ルールを示す識別子を、デジタルインターフェースD-I/F78を介して、デジタルAVデータ送信ユニットSTB56に送る。ユニット認証ルール情報受信手段60が、単一認証デジタルAVデータ受信ユニットVTR72から送られてきた認証ルールに関する情報、つまり共通鍵による認証ルールの識別子を、デジタルインターフェースD-I/F62を介して、受け取り、さらにこの認証ルールの識別子は、送信側認証ルール取り出し手段58に渡される。送信側認証ルール取り出し手段58は、送信側複数認証ルール格納手段63から、その認証ルールに関する情報に応じた認証ルール、つまり共通鍵による認証ルールを取り出し、送信側認証手段61に渡す。送信側認証手段61と受信側認証手段77は互いに、デジタルインターフェースD-I/F62とD-I/F78を介して、認証を交わす。認証が成功すれば、その結果、第一の実施の形態で詳述したごとく、送信側にワーク鍵Kco79、受信側にワーク鍵Kco81が生成される。認証の結果ワーク鍵が生成される過程は、第一の実施の形態で詳述した。

【0068】データ82は暗号化手段64にてワーク鍵Kco79により暗号化される。暗号化されたデータはデジタルインターフェースD-I/F62を介して、単一認証デジタルAVデータ受信ユニットVTR72に送られる。デジタルインターフェースD-I/F78を介して受信した暗号化されたデータは、復号化手段73に送られ、ワーク鍵Kco81を用いて復号化され、データ84が得られる。これはデータ82と同一のデータであ

り、デジタルAVデータ送信ユニットSTB56から、単一認証デジタルAVデータ受信ユニットVTR72にデータが送信されたことになる。

【0069】次に、本発明の第四の実施の形態を説明する。

【0070】本実施の形態では、デジタルAVデータ受信ユニットが正当なものか不正なものかを調べて作成しておいた管理基準(CRL)を利用するものである。そのCRLの作成の仕方は、例えば、消費者が購入した販売店が発行した登録カードを元に作成する方法等が考えられる。

【0071】図8は、その管理基準を放送局から送られてくるデジタルAVデータの重要度に応じて、その管理基準を参照するかどうか決定するものである。

【0072】デジタルAV送信ユニットSTB93は、放送局から送られてくるデジタルAVデータの重要度に応じて、データの重要性を判定する、データ重要性判定手段86を有する。また、データの重要度に応じて管理基準格納手段88に格納されている管理基準情報(CRL)を参照するかどうかを判定する、管理基準参照決定手段87を有する。また、前記決定結果に従って、認証を行うかどうかを決定する、認証決定手段89を有する。また、実際にデジタルAVデータ受信ユニットTV92と認証を交わす、認証手段90を有する。前記認証手段90は、デジタルインターフェースD-I/F91を介して、デジタルAVデータ受信ユニットTV92に接続している。

【0073】次に本実施の形態の動作を説明する。まず、放送局から送られてくるデジタルAVデータ85は、データ重要性判定手段86で、重要性を判定される。その結果は、管理基準参照決定手段87に渡され、管理基準格納手段88に格納されている情報を参照すべきかどうか決定される。例えば、新作の映画等の場合は重要なので、管理基準情報を参照すると決定する。また、ニュース等の場合は重要でないので、管理基準情報を参照しないと決定する。さらに認証決定手段89で、前記管理基準参照決定手段87の判定決定に従って、認証すべきかどうか決定される。すなわち、デジタルAVデータ受信ユニットTV92が、デジタルAVデータ85を受信するのに正当な機器か不当な機器かを、管理基準格納手段88に格納されている管理基準情報で判断される。正当であると判断されれば、次の認証手段90で、デジタルインターフェースD-I/F91を介して、デジタルAV受信ユニットTV92と認証が交わされる。不当と判断されればその時点で、デジタルAVデータ受信ユニットTV92との認証は交わされず、データ85の送信はされない。

【0074】他方、図9は上述した管理基準を、デジタルAVデータ受信ユニットの装置の種類、あるいは重要度に応じて、その管理基準を参照するかどうか決定する

ものである。

【0075】デジタルAVデータ送信ユニットSTB94は、デジタルAVデータ受信ユニットVTR100の装置の種類あるいは、重要度に応じて、その管理基準格納手段96を参照すべきかどうかを決定する、管理基準参照決定手段95を有する。また、認証決定手段97は、認証するかどうかを決定する。管理基準格納手段96は、デジタルAVデータ受信ユニットVTR100がデジタルAVデータを受信するのに正当な機器か正当でない機器かの情報が格納されている。認証手段98は、

デジタルインターフェースD-I/F99を介して、デジタルAVデータ受信ユニットVTR100と認証を行う。

【0076】次に本実施の形態の動作を説明する。まず、デジタルAVデータ受信ユニットVTR100が、デジタルインターフェースD-I/F99を介して、管理基準参照決定手段95に機器情報を送る。これを受けて、管理基準参照決定手段95は、管理基準格納手段96に格納されている情報を参照すべきかどうかを決定する。管理基準格納手段96を参照すると決定された場合は、認証決定手段97は、まず、管理基準格納手段96を参照して、デジタルAVデータ受信ユニットがデータを受信するのに正当な機器か、不正な機器かを判定する。ここで、正当な機器と判定されれば、次の認証手段98にて、デジタルインターフェースD-I/F99を介して、デジタルAVデータ受信ユニットと認証を開始する。デジタルAVデータ受信ユニットがデータを受信するのに不正な機器と判定された場合は、認証は行われず、データの送信も行われない。

【0077】なお、上記実施の形態では、STBを送信ユニットとして説明してきたが、VTRで録画したデータを再生する際には、VTRが送信ユニットとなる。この際CGMSが入力時「1回コピー可」であれば「コピー不可」に書き換えられて出力される。ここで、データの重要度としては、元の入力時における重要度と考えるべきであり、「1回コピー可」と同様の認証ルールを使うこともできる。このように「1回コピーの結果コピー不可となったデータ」と「元からコピー不可のデータ」を見分ける必要がある際には、前述した、存在しないCGMS値01を前者の区別用に割り当てることが出来る。

【0078】次に本発明の第五の実施の形態について説明する。

【0079】図10は、本発明の第五の実施の形態についての概略図である。本実施の形態では、認証手続きのレベル2段階、コンテンツの重要度、すなわち、解読情報としての暗号鍵を3種類としている。図10において、デジタルAVデータ送受信システムは、送信ユニット111と、それに接続された受信ユニット130により構成されている。

【0080】送信ユニット111は、コンテンツ重要度が異なるデータA、Bを各々異なる暗号鍵Kcoで暗号化する暗号化手段A、B112、113と、暗号化用の例えば、copy_never（テープ等に記録してはいけないコンテンツ）用Kco、copy_once（一度だけ記録してもよいコンテンツ）用Kco、no_more_copy（これ以上コピーしてはならないコンテンツ）用Kcoを記憶するKco記憶手段114と、受信ユニット130に渡す、'Exchange_Key'と呼ばれるcopy_never用、copy_once用、no_more_copy用の各暗号鍵Kexを発生するKex発生手段115と、その発生した各Kexを記憶するKex記憶手段116と、暗号化用鍵Kcoを所定の関数により算出する時に用いる種を発生する種発生手段117と、その発生した種を記憶する種記憶手段118と、Kex記憶手段116からのKexと種記憶手段118からの種を用いて、関数 $K_{co} = f(\text{種}, K_{ex})$ によりKcoを算出するKco算出手段119と、受信ユニット130に対して認証手続きを実行する認証手段121と、受信ユニット130の認証済みのレベルを判定する等の処理を行うレベル判定手段122と、受信ユニット130からの種要求に対して応答する種要求コマンド応答手段120と、データの送受信を行うデジタルインターフェース（D-I/F）123により構成されている。ここで、種要求コマンド応答手段120及び認証手段121の一部などが解読情報選択手段を構成している。

【0081】また、受信ユニット130は、データの送受信を行うデジタルインターフェース（D-I/F）131と、受信した暗号化デジタルAVデータのコンテンツの重要度に応じて、要求する認証のレベルを決定する要求レベル決定手段134と、その決定された要求レベルで、送信ユニット111に認証を要求し、必要な暗号鍵Kexを取得する認証手段133と、その取得したKexを記憶するKex記憶手段137と、種の要求コマンドを発行し、種を送信ユニット111から取得する種要求コマンド発行手段135と、その取得した種とKex記憶手段137に記憶されたKexとを用いて、送信ユニット111と同一の関数 $K_{co} = f(\text{種}, K_{ex})$ によりKcoを算出するKco算出手段136と、その算出したKcoにより暗号化データを復号する復号化手段132により構成されている。ここで、種要求コマンド発行手段135及び認証手段133の一部などが解読情報要求手段を構成している。

【0082】次に、上記実施の形態のデジタルAVデータ送受信システムの動作について、図面を参照しながら説明する。

【0083】図11において、まず、受信ユニット130では、要求レベル決定手段134が受信データのコンテンツ重要度に基づいて要求する認証のレベルを決定し、認証手段133に渡す。認証手段133はD-I/F

F131を介して送信ユニットに認証要求を出す。ここでは、一番高いレベルの認証を要求するものとする。送信ユニット111では、D-1/F123を介して受け取った認証要求に基づいて認証処理を行う。認証の方法については、例えば前述した実施の形態で説明した方法等により行うことができ、このとき送信ユニット、受信ユニットともに共有の共通鍵K_{ab}が得られる。又、このときの認証済みのレベルがレベル判定手段122に渡される。

【0084】次に、認証が完了してその通知が受信ユニット130に送信されると、認証手段133は、認証レベルが最高であることから、送信ユニット111に対して全てのレベルのK_{ex}を要求する。ここでは、K_{ex}のレベルとして、高い順にcopy_never用(K_{ex}1)、copy_once用(K_{ex}2)、no_more_copy用(K_{ex}3)の3種類とする。

【0085】送信ユニット111では、レベル判定手段122が、認証手段121から受けた要求レベルを認証済みレベルに基づいて判定し、渡せるか否かの判定と、渡せる場合は、要求のあったK_{ex}(このときは、K_{ex}1、K_{ex}2、K_{ex}3)を両者が共有するK_{ab}で暗号化して、認証手段121を通じて受信ユニット130に送信する。受信ユニット130では、認証手段133が暗号化されたK_{ab}(K_{ex}1、K_{ex}2、K_{ex}3)を自身の持つK_{ab}で復号してK_{ex}記憶手段137に記憶する。

【0086】一方、K_{ex}発生手段115が発生した各レベルのK_{ex}、すなわち、K_{ex}1、K_{ex}2、K_{ex}3は、K_{ex}記憶手段116に記憶され、種発生手段117が発生した種は、種記憶手段118に記憶されている。又、K_{ex}記憶手段116に記憶された各K_{ex}と、種記憶手段118に記憶された種とを用いて、K_{co}算出手段119が各K_{co}、すなわち、copy_never用(K_{co}1)、copy_once用(K_{co}2)、no_more_copy用(K_{co}3)を算出してK_{co}記憶手段114に記憶している。更に、暗号化手段A、B112、113は、各データのコンテンツの重要度に対応したK_{co}を用いてデジタルAVデータを暗号化して受信ユニット130に送信する。

【0087】受信ユニット130では、種要求コマンド発行手段135が種要求コマンドを送信ユニット111に送信する。そうすると、送信ユニット111では、種要求コマンド応答手段120が、種記憶手段118から種を取り出し受信ユニット130に送信する。ここで、図の種記憶手段118に現在の種及び次の種とあるのは、暗号化用のK_{co}を刻々と変更しているためである。

【0088】次に、受信ユニット130では、種要求コマンド発行手段135が送信ユニット111から受け取った種と、K_{ex}記憶手段に記憶している復号化するデータのレベルに対応するK_{ex}とを用いて、K_{co}算出手段136は、送信ユニット111と同一の関数(この関数

は、送信ユニット及び受信ユニットが予め持っており、第3者は入手できないものとする)によりK_{co}を算出する。復号化手段132はこの算出されたK_{co}を用いて暗号化されたデジタルAVデータを通常のデジタルAVデータに復号する。ここで、利用するデータが、コンテンツ重要度の高いデータ1(例えば、映画など)から低いデータ2(例えば、スポーツ番組など)に変化、あるいは変更する場合は、最初に受け取った各K_{ex}の中から、必要なK_{ex}を選択してK_{co}を算出して用いることができるので、新たな認証手続きは勿論、K_{ex}の要求もする必要が無い。

【0089】前述の方法は、認証手続きに続いて入手可能な全てのK_{ex}を一度に取得する方法であったが、図12に示すような方法を用いてもよい。

【0090】図12において、まず、受信ユニット130では、要求レベル決定手段134が受信データのコンテンツ重要度に基づいて要求する認証のレベルを決定し、認証手段133に渡す。認証手段133はD-1/F131を介して送信ユニットに認証要求を出す。ここでは、一番高いレベルの認証を要求するものとする。送信ユニット111では、D-1/F123を介して受け取った認証要求に基づいて認証処理を行う。認証の方法については、例えば前述した実施の形態で説明した方法等により行うことができ、このとき送信ユニット、受信ユニットともに共有の共通鍵K_{ab}が得られる。又、このときの認証済みのレベルがレベル判定手段122に渡される。

【0091】次に、認証が完了してその通知が受信ユニット130に送信されると、認証手段133は、送信ユニット111に対して認証レベルが一番高いK_{ex}を要求する。ここでは、K_{ex}のレベルとして、高い順にcopy_never用(K_{ex}1)、copy_once用(K_{ex}2)、no_more_copy用(K_{ex}3)の3種類とする。

【0092】送信ユニット111では、レベル判定手段122が、認証手段121から受けた要求レベルを認証済みレベルに基づいて判定し、渡せるか否かの判定と、渡せる場合は、要求のあったK_{ex}(このときは、K_{ex}1)を両者が共有するK_{ab}で暗号化して、認証手段121を通じて受信ユニット130に送信する。受信ユニット130では、認証手段133が暗号化されたK_{ab}(K_{ex}1)を自身の持つK_{ab}で復号してK_{ex}記憶手段137に記憶する。

【0093】次に、受信ユニット130では、種要求コマンド発行手段135が種要求コマンドを送信ユニット111に送信する。そうすると、送信ユニット111では、種要求コマンド応答手段120が、種記憶手段118から種を取り出し受信ユニット130に送信する。

【0094】種を受信した受信ユニット130では、種要求コマンド発行手段135が送信ユニット111から

受け取った種と、K_{ex}記憶手段に記憶している復号化するデータのレベルに対応するK_{ex} (K_{ex1}) とを用いて、K_{co}算出手段136は、送信ユニット111と同一の関数(この関数は、送信ユニット及び受信ユニットが予め持っており、第3者は入手できないものとする)によりK_{co} (K_{co1}) を算出する。復号化手段132はこの算出されたK_{co1} を用いて暗号化されたデジタルAVデータを通常のデジタルAVデータに復号する。ここで、利用するデータが、コンテンツ重要度の高いデータ1から低いデータ2に変化、あるいは変更する場合は、別のK_{ex} (図ではK_{ex2}) を送信ユニット111に対して要求する。

【0095】送信ユニット111では、レベル判定手段122が認証手段121を介して、要求されたK_{ex}のレベルを認証済みのレベルに基づいて判定し、認証済みレベルと同等か、あるいはそれより低いレベルの要求であれば、要求されたK_{ex} (K_{ex2}) をK_{ab}で暗号化して受信ユニット130に送信する。

【0096】ここで、受信ユニット130が、最初の認証要求を行って認証が完了した場合に、その認証済みのレベル(認証済みのレベルのうち最高のレベルのものでよい)を記憶しておき、次回からのK_{ex}の要求に対しては、その記憶した認証済みのレベルから所望するK_{ex}が認証無しに入手可能か否かを、例えば認証手段133で判断して入手可能であればK_{ex}を要求するようにしてもよい。このとき、入手不可能である場合は、更に、新たな高いレベルの認証を行うようにすればよい。従って、要求レベル決定手段134で、デジタルAVデータのコンテンツ重要度に基づいて決定された要求レベルが、記憶されている過去の認証済みレベルと同等かあるいはそれ以下のレベルである場合に、認証手段133から所望のK_{ex}を要求する。

【0097】また、送信ユニット111側については、もし、認証要求がなくK_{ex}の要求があつて、要求されたK_{ex}が送信不可と判定された場合に、新たな認証が必要である旨の情報を受信ユニット130側に通知する方法としてもよい。

【0098】受信ユニット130では、認証手段133がK_{ab} (K_{ex2}) を復号してK_{ex}記憶手段137に記憶し、K_{co}算出手段136がそのK_{ex2}及び種を用いてK_{co2}を算出してデータを復号する。この方法によると、1度あるレベルでの認証が済んでいれば、そのレベルと同等か、あるいはそれ以下のレベルのK_{ex}を取得する場合、新たに認証手続きを行う必要が無いので、時間のかかる認証手続きの回数を減少することになる。

【0099】ところで、従来のように、コンテンツの重要度の異なるAVデータを利用したい場合に、その都度認証手続きを行う方法では、受信ユニットが多数接続されているときは、認証要求の頻度が増大する。しかしながら、認証要求のための通信は、例えば、IEEE13

94BUS規格のようなアイソクロナスデータ通信とアシンクロナスデータ通信とを用いるものでは、本来データの通信帯域に使う帯域の一部を用いて行っているため、時間のかかる認証要求の頻度が増大することは好ましくない。従って、本実施の形態によれば、受信ユニットの台数が増えても、基本的には1受信ユニットについて1回の認証手続きで済むので、認証要求による不都合が生じない。

【0100】なお、上記第五の実施の形態では、認証手続きのレベルを2段階としたが、これに限定されるものではない。

【0101】また、上記第五の実施の形態では、コンテンツの重要度のレベルを3種類としたが、これに限定されるものではない。例えば、copy_free(何度でも記録してよいコンテンツ)のレベルを加えて4種類としてもよいし、それ以上の種類としてもよい。

【0102】また、上記第五の実施の形態では、種と暗号鍵とを用いて関数により暗号化用の鍵を算出する方法により実現する構成としたが、これに限らず、他の実施の形態で説明した方法を用いた構成に適用してもよい。

【0103】また、上記第五の実施の形態では、受信中のデータの重要度を見て、要求するK_{ex}の種類を決定しているが、予め自分が受信する可能性のある全てのK_{ex}を取得しておいてもよい。

【0104】また、上記第五の実施の形態では、認証を行った後に、受信ユニットがK_{ex}の要求を行うとしたが、これに限定されない。例えば、認証要求をする際に、同時に自分が受け取りたいK_{ex}の種類を送信ユニットに対して申請し、認証が完了した時点で、送信ユニットが自動的に要求されたK_{ex}を受信ユニットに送信してもよい。

【0105】また、上記第五の実施の形態では、データの重要度に応じて暗号鍵を替える方法であったが、これに限らず、データの種類等に応じて暗号鍵を替えるようにしてもよい。その場合は、認証のレベルとデータの種類(すなわち、暗号鍵)を対応させておく必要がある。

【0106】次に本発明の第六の実施の形態について説明する。

【0107】図13は、本発明の第六の実施の形態についての概略図である。本実施の形態は、Full認証とRestricted認証(以下、Rest認証と略称する)機能を備えたデジタルAVデータ送信ユニット140には、Rest認証機能のみを持つデジタルAVデータ受信ユニット150及びFull認証とRest認証の両機能を備えたデジタルAVデータ受信ユニット160が接続されているものとする。ここで、Full認証とは、例えば公開鍵と秘密鍵とを用いた高レベルの認証方法であり、Rest認証とは、例えば共通鍵を用いた通常の認証方法を示すものとする。

【0108】図13において、デジタルAVデータ送信

ユニット140は、データを暗号化する暗号化手段141、Full認証用のルールを格納するFull認証格納手段143、Rest認証用のルールを格納するRest認証格納手段142、管理基準としてのCRL (Certification Revocation List: 不正機器の排除を行うための不正機器リスト) を格納するCRL格納手段144、受信ユニットからの認証要求を受けて認証ルールを選択する送信側認証選択手段147、その送信側認証選択手段147の選択結果に
10 応じて、Full認証とRest認証を切り替える切替手段148、切り替えられて選択された認証ルールにより受信ユニットとの間で認証を行う認証手段146、及び受信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うD-I/F (デジタルインターフェース) 145から構成されている。CRLは入力データに付加されて新しい内容に随時更新される。

【0109】一方、デジタルAVデータ受信ユニット150は、送信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うD-I/F 151、送信ユニットから受信した暗号化データを復号化する復号化手段
20 152、送信ユニットに対して認証要求を行う認証要求手段153、及びRest認証ルールにより認証を行う認証手段154から構成されている。

【0110】また、デジタルAVデータ受信ユニット160は、送信ユニットとの間で暗号化データや認証要求など情報のやり取りを行うD-I/F 161、送信ユニットから受信した暗号化データを復号化する復号化手段162、送信ユニットに対して認証要求を行う認証要求手段163、Full認証用のルールを格納するFull
30 認証格納手段166、Rest認証用のルールを格納するRest認証格納手段165、認証要求手段163からの指示により認証ルールを切り替える切替手段167、及び切り替えられ選択された認証ルールにより認証を行う認証手段164から構成されている。

【0111】次に、上記実施の形態の動作について図面を参照しながら説明する。

【0112】まず、前述のCRLは、管理センターから送られてくるが、入手するには、Full認証の機能を利用する。そのため、Rest認証機能のみを持つ機器では、CRLを入手できない。従って、Rest認証機能のみを持つ機器側は、CRLチェックによる機器排除を行えない。ここで、送信ユニット及び受信ユニットがともにFull認証及びRest認証機能を有する場合
40 について、CRLチェックを用いた手順を説明する。

【0113】図15は、図4に示した公開鍵及び秘密鍵による認証方法に、CRLチェックを付加したものである。

【0114】図15において、送信側には、管理センター (ライセンス機構) からそのユニットの識別用のIDa、及びそのIDaに対する署名Aが送られ、受信側に
50

は、管理センターからそのユニットの識別用のIDb、及びそのIDbに対する署名Bが送られているものとする。また、この場合受信側は秘密鍵Sbと公開鍵Pbを持つ。また送信側は秘密鍵Saと公開鍵Paを持つ。

【0115】まず、ステップ41で受信側が乱数Bを発生する。受信側は自己の認識番号であるIDb及び署名Bと、乱数Bを自らの秘密鍵Sbで暗号化した暗号文Sb (B) を送信側へ送る。送信側は受信側の認識番号IDbから検索して受信側の公開鍵Pbを入手する。ステップ49で、入手した公開鍵Pbで暗号文Sb (B) を復号化する。その結果ステップ50のごとく乱数Bが得られる。さらに、送信側は、ステップ51で、受信側のIDbに対してCRLチェックを行う。すなわち、IDbがCRLに無いかどうかを調べ、無ければステップ52で乱数Aを発生する。CRLに有れば不正機器であるとして認証を中止する。ステップ52で、乱数AとBは送信側の秘密鍵Saで暗号化され暗号文Sa (A, B) が作成される。送信側は暗号文Sa (A, B) と自己の認識番号IDaを受信側へ送信する。受信側は、暗号文Sa (A, B) と送信側の認識番号IDaを受け取り、送信側の認識番号IDaから検索して送信側の公開鍵Paを入手し、ステップ42のごとく、Paで暗号文Sa (A, B) を復号化する。ここで、暗号文Sa (A, B) から受信側にはステップ41で送った乱数Bと全く同一の乱数Bが得られ、偽造や改竄が行われてないことが受信側にわかる。もし前記2つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。但し、この場合は、公開鍵Pa, Pbは正当な者にしか入手できないようになっているものとする。次に受信側はステップ43のごとく、受信側の秘密鍵Sbで乱数Aを暗号化し、暗号文Sb (A) を作成する。Sb (A) は送信側へ送られ、ステップ53のごとく既に送信側で持っている、受信側の公開鍵Pbで暗号文Sb (A) を復号化する。ステップ52で発生した、乱数Aとステップ53で復号化した乱数Aが全く同一であれば、偽造や改竄が行われていないことが送信側にわかる。もし前記2つの乱数が異なっていれば、偽造や改竄が行われたことがわかり不正な相手がいることがわかる。

【0116】一方、受信側は、ステップ44で送信側のIDaに対してCRLチェックを行う。そして、IDaがCRLに有れば認証を中止し、無ければ次のステップに移る。今、送信側及び受信側でのCRLチェックの結果が異常が無く、受信側と送信側でやりとりした乱数AとBは偽造や改竄が行われていないとすると、受信側と送信側以外の第3者には乱数AとBは秘密の乱数である。そこで送信側で、ステップ54のごとく、乱数AとBを用いて鍵Kabを作成する。同じくステップ45のごとく受信側で乱数AとBを用いて鍵Kabを作成する。前記2つのKabは全く同一のものであり共通鍵と
50

なっている。次に送信側でステップ55のごとく鍵 K_{ex} を作成する。これを共通鍵 K_{ab} で暗号化し、暗号文 $K_{ab}(K_{ex})$ を作成して、受信側に送る。受信側はステップ46のごとく共通鍵 K_{ab} で暗号文 $K_{ab}(K_{ex})$ を復号化して K_{ex} を得、その結果、受信側が得た鍵 K_{ex} と送信側にある鍵 K_{ex} は全く同一であり、共通鍵となる。次に送信側でステップ56のごとく鍵 K_{co} を作成する。鍵 K_{co} は共通鍵 K_{ex} で暗号化され、暗号文 $K_{ex}(K_{co})$ として、受信側に送られる。受信側では、ステップ47のごとく共通鍵 K_{ex} で暗号文 $K_{ex}(K_{co})$ を復号化し、ステップ48のごとく K_{co} を得る。送信側にある鍵 K_{co} と受信側にある K_{co} は全く同一で、共通鍵となっている。以上が公開鍵と秘密鍵による認証の過程で得られたワーク鍵 K_{co} である。

【0117】上記説明では、CRLチェックをステップ52の乱数Aの発生の前に行ったが、IDb受信後であれば、どこで行ってもよい。規格上はKABを作成するステップ54の後に行う。

【0118】次に、受信側がRest認証機能のみの場合について説明する。この共通鍵による認証を行う場合は、前述したような方法を用いることはできない。そこで、受信側にそのユニットに対するCRL用のIDとそのIDを用いて作成された署名を付与し、送信側でCRLを利用する方法を用いる。

【0119】図14において、受信側には、管理センターから受信ユニットのIDb及び署名Bが与えられ、送信側と受信側は共通鍵Sを持つ。なお、この共通鍵は正当な者にしか与えられていない。まず、受信側でステップ30のごとく2個の乱数A1、A2を発生し、共通鍵Sで暗号化し、暗号文S(A1A2)を作成し、IDb及び署名Bとともに送信側へ送る。送信側ではステップ35のごとく共通鍵Sで暗号文S(A1A2)を復号化する。そして、受信側のIDbに対してCRLチェックを行う。また、署名Bもチェックする。このとき、CRLチェック及び署名Bのチェックのどちらか一方でも異常が有る場合は、認証を中止する。CRLチェック及び署名Bのチェックの結果が両方とも正常であれば、ステップ37のごとく乱数A1と乱数A2が得られる。送信側は乱数A2を受信側に送る。受信側はステップ31のごとく2つの乱数A1とA2を持つことになる。ステップ30で発生した乱数A2とステップ31で送信側から受け取った乱数A2が全く同じであれば、送信側で偽造や改竄が行われていないことがわかる。もし、上記2つの乱数が異なっていれば偽造や改竄が行われたことになり認証は失敗する。次に送信側はステップ38のごとく乱数B1とB2を発生し、暗号化して、暗号文S(B1B2)を受信側に送る。受信側はステップ32のごとく共通鍵Sを用いて暗号文S(B1B2)を復号化する。すると、ステップ33のごとく乱数B1とB2が得られる。受信側は乱数B2を送信側に送る。送信側はステッ

プ39のごとく乱数B1とB2を持つことになる。ステップ38で発生した乱数B2と、ステップ39で受信側から受け取った乱数B2が同じであれば、受信側に、偽造や改竄が行われていないことがわかり、認証は成功する。もし、上記2つの乱数が異なっていれば、偽造や改竄が行われたことになり認証は失敗である。

【0120】ここまでで、認証が成功しているとする。と、乱数A1と乱数B1は送信側と受信側以外の第3者には秘密の乱数である。送信側ではステップ40のごとくIDb及び乱数A1と乱数B1から鍵 K_{co} を作成する。一方受信側では、ステップ34のごとくIDb及び乱数A1と乱数B1から鍵 K_{co} を作成する。送信側にある鍵 K_{co} と受信側にある鍵 K_{co} は全く同一であり、共通鍵となっている。以上が共通鍵による認証の過程で得られたワーク鍵 K_{co} である。この方法によれば、IDbと署名Bが対応しているので、IDbが盗まれて送信側でのCRLチェックがパスしても、署名Bによるチェックで不正使用が防止できる。

【0121】ここで、CRL用のIDは、例えば40ビットのデバイスIDを使用する。これにより、Full認証、Rest認証に関わらずすべての1394CPデバイスが40ビットのデバイスIDを持つことになる。

【0122】なお、上記の説明では、管理センターでの署名の作成を、IDを用いて作成したが、このIDは管理センターが任意に決めるものである。さらに、安全性を高めるために、機器を製作する時に予め機器毎に埋め込まれる機器固有の識別子であるNUIDを用いる。すなわち、受信側は管理センターに申請する際に、その機器のNUIDを知らせ、管理センターは、そのNUIDとCRL用のIDを用いて署名を作成し、CRL用のIDと署名を受信側に付与する。

【0123】また、上記実施の形態では、認証ルールの種類をFullとRestの2種類としたが、認証ルールの種類はこれに限定されるものではなく、3種類以上であっても、受信側がCRLを持てない機器構成の場合は、前述と同様に適用可能である。

【0124】また、本発明の各構成要素は、それぞれの機能を実現する専用のハード回路、機器等で実現しても、あるいは、コンピュータを利用してソフトウェア的に実現してもかまわない。

【0125】また、本発明をコンピュータで実現する場合、それらの各構成要素の機能の全部又は一部を実現するためのプログラムを格納した媒体も本発明に属する。

【0126】

【発明の効果】以上説明したところから明らかなように、本発明は、重要でないデータの認証に多くの時間を要せず、重要なデータに関しては、その認証が偽造や改竄に強くまた、ユニットによって認証に必要な厳密さを変えることによって、データの重要性や相手の装置が有する認証方法の種別などを考慮して、適切な認証方法で

データの送受信を行いうるユニット、システム等を提供することができる。

【0127】また、本発明は、コンテンツの重要度に応じた複数種類の解読情報を得る場合に、認証回数を減少することができるという利点がある。

【0128】また、本発明は、排除機能を持たない受信機器であっても、送信側で機器の排除を行うことが可能となる。

【図面の簡単な説明】

【図1】本発明の第一の実施の形態についての概略図

【図2】従来技術について示す概略図

【図3】従来技術について示す概略図

【図4】本発明の実施の形態のうち認証方法に関するブロック図

【図5】本発明の実施の形態のうち認証方法に関するブロック図

【図6】本発明の第二の実施の形態についての概略図

【図7】本発明の第三の実施の形態についての概略図

【図8】本発明の第四の実施の形態についての概略図

【図9】本発明の第四の実施の形態についての概略図

【図10】本発明の第五の実施の形態についての概略図

【図11】同第五の実施の形態における手順方法の一例を示す図

【図12】同第五の実施の形態における手順方法の別の一例を示す図

【図13】本発明の第六の実施の形態についての概略図

【図14】同第六の実施の形態における手順方法の一例を示す図

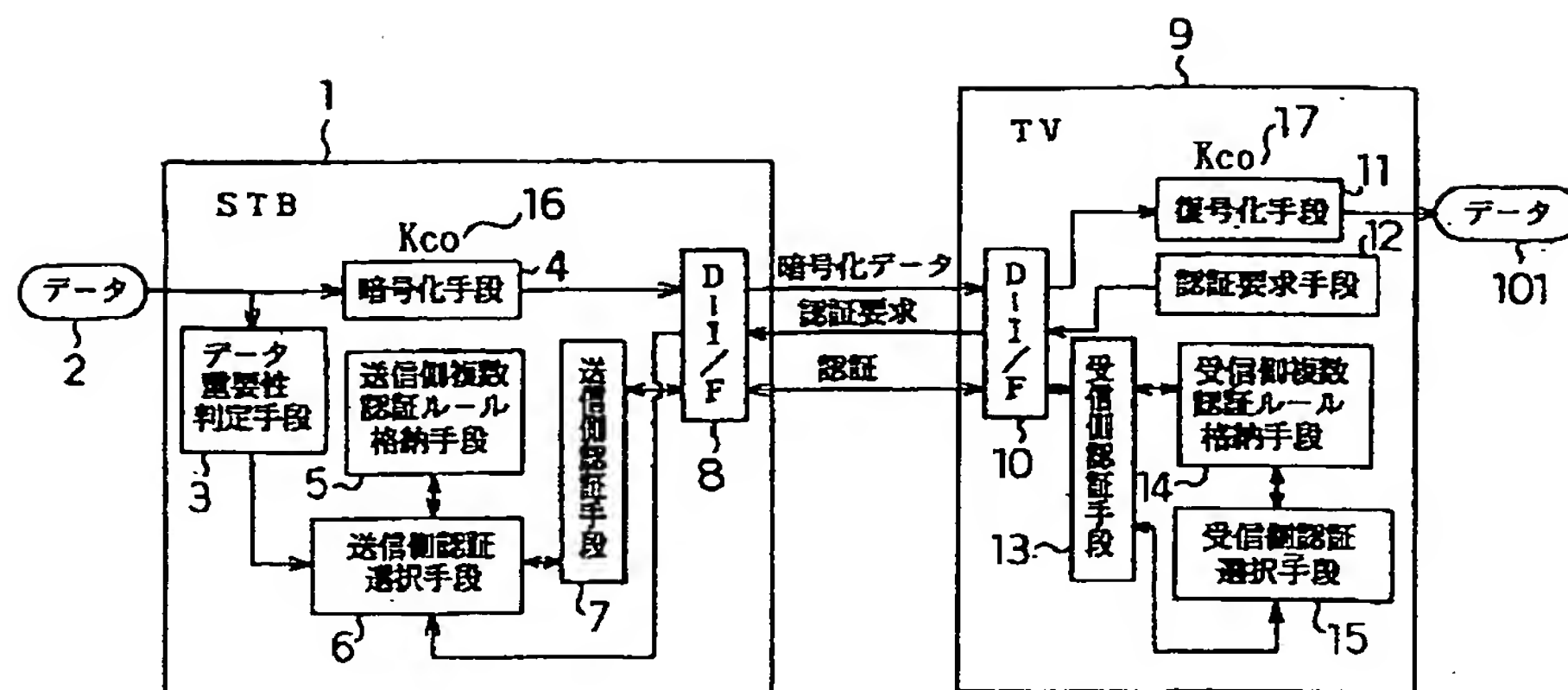
【図15】送信側及び受信側両方でCRLチェックを行う場合の手順方法の一例を示す図

【符号の説明】

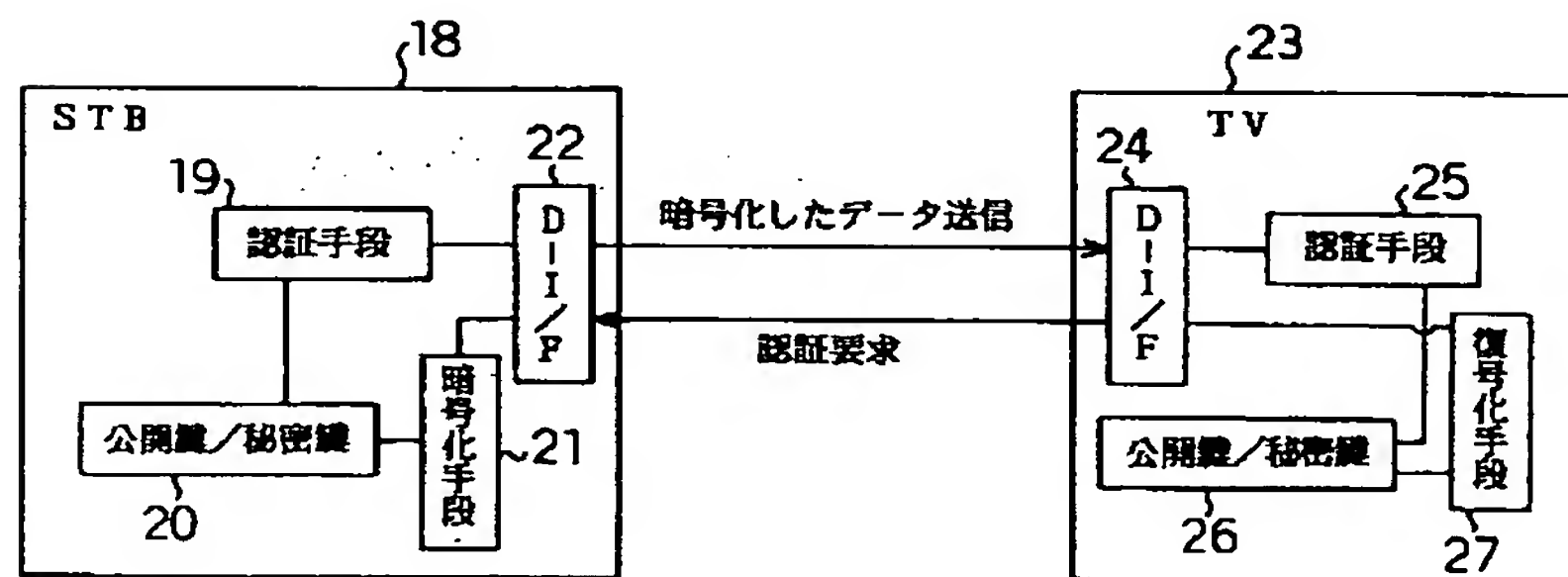
- 1 STB
- 3 データ重要性判定手段
- 5 送信側複数認証ルール格納手段
- 6 送信側認証選択手段
- 7 送信側認証手段
- 9 TV
- 13 受信側認証手段
- 14 受信側複数認証ルール格納手段
- 15 受信側認証選択手段
- 18 STB
- 19 認証手段
- 20 公開鍵／秘密鍵
- 23 TV
- 25 認証手段
- 26 公開鍵／秘密鍵
- 28 STB

- 29 認証手段
- 30 共通鍵
- 33 TV
- 35 認証手段
- 36 共通鍵
- 38 STB
- 41 送信側複数認証ルール格納手段
- 42 ユニット認証ルール情報受信手段
- 43 送信側認証手段
- 45 VTR
- 48 認証要求手段
- 49 受信側認証ルール格納手段
- 50 認証ルール情報送信手段
- 51 受信側認証手段
- 55 送信側認証ルール取り出し手段
- 56 STB
- 57 データ重要性判定手段
- 58 送信側認証ルール取り出し手段
- 59 送信側認証選択手段
- 60 ユニット認証ルール情報受信手段
- 61 送信側認証手段
- 63 送信側複数認証ルール格納手段
- 65 TV
- 67 認証要求手段
- 68 受信側複数認証ルール格納手段
- 69 受信側認証選択手段
- 70 受信側認証手段
- 72 VTR
- 74 認証要求手段
- 75 受信側認証ルール格納手段
- 76 認証ルール情報送信手段
- 77 受信側認証手段
- 86 データ重要性判定手段
- 87 管理基準参照決定手段
- 88 管理基準格納手段
- 89 認証決定手段
- 90 認証手段
- 92 TV
- 93 STB
- 94 STB
- 95 管理基準参照決定手段
- 96 管理基準格納手段
- 97 認証決定手段
- 98 認証手段
- 100 VTR
- 144 CRL格納手段

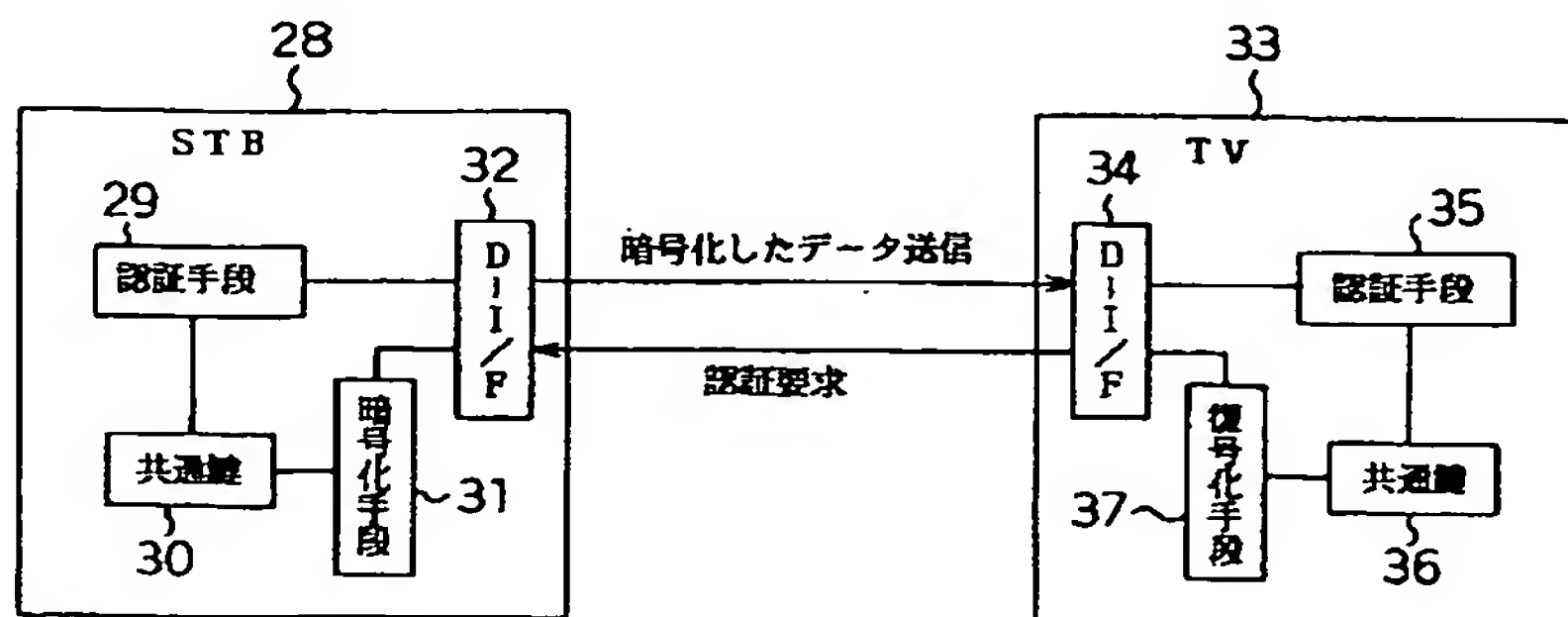
【図1】



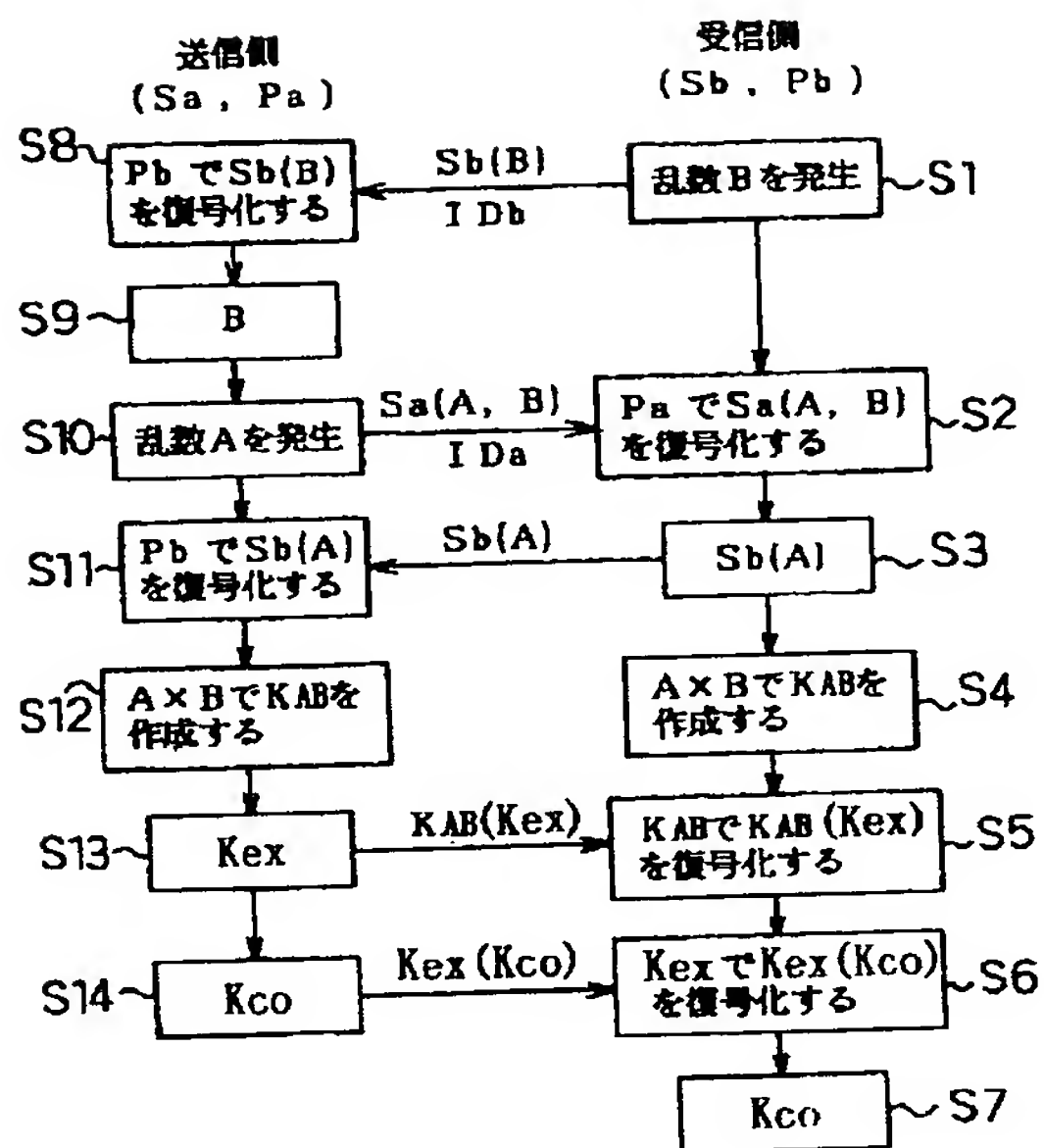
【図2】



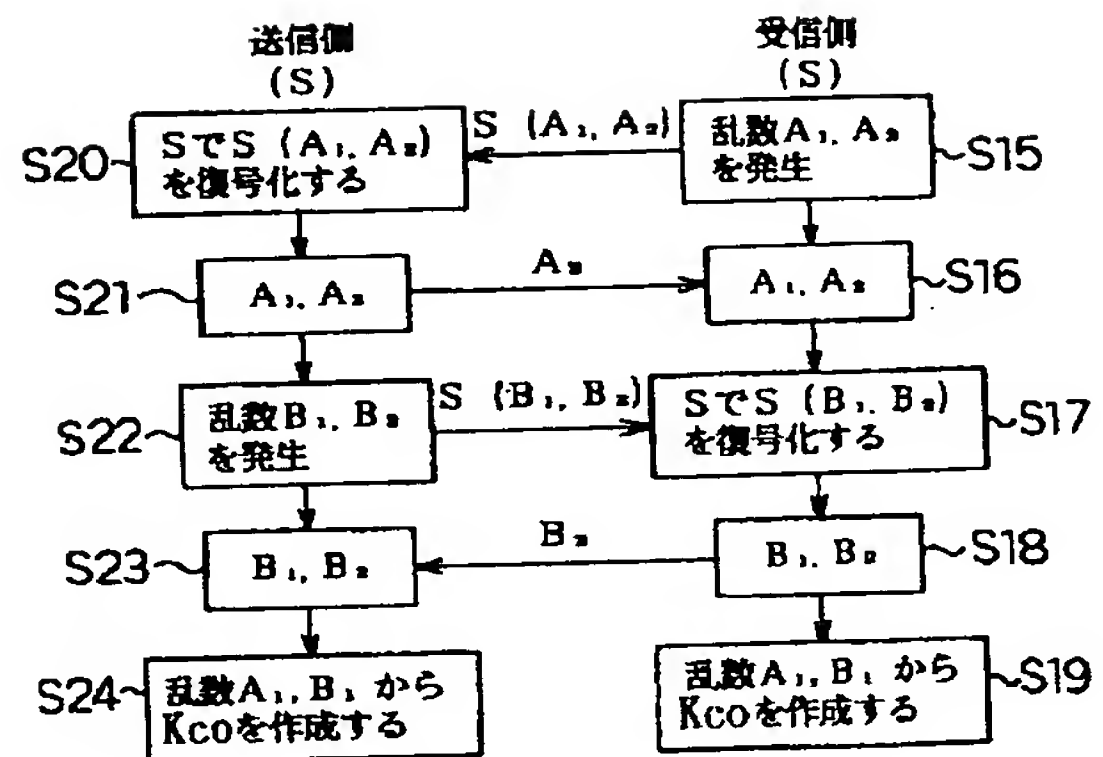
【図3】



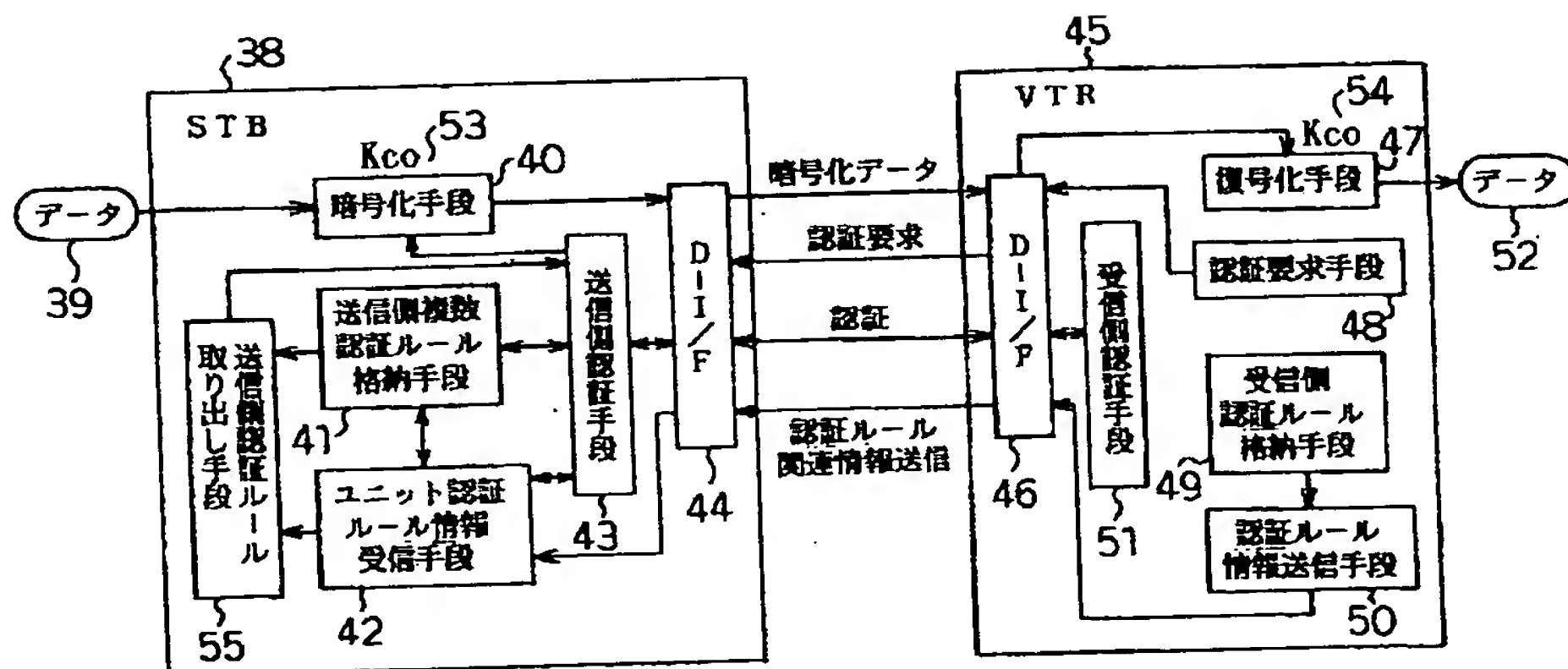
【図4】



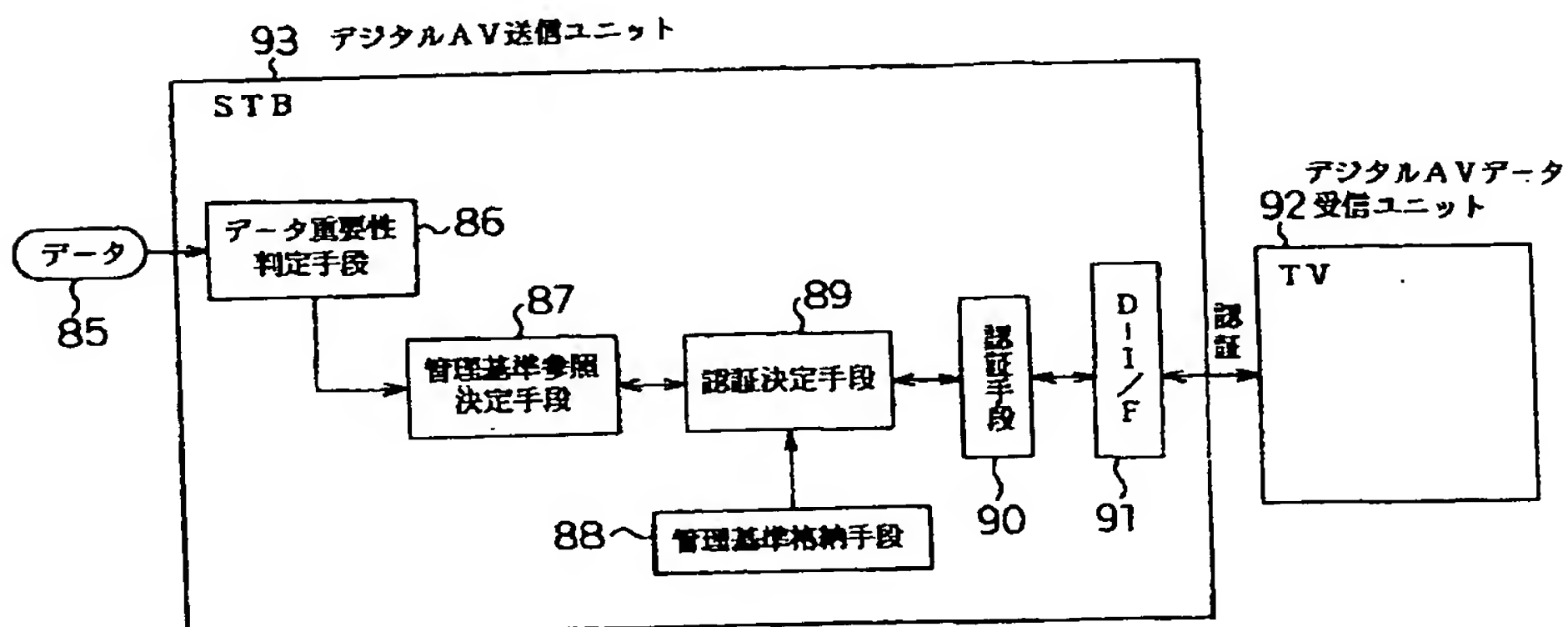
【図5】



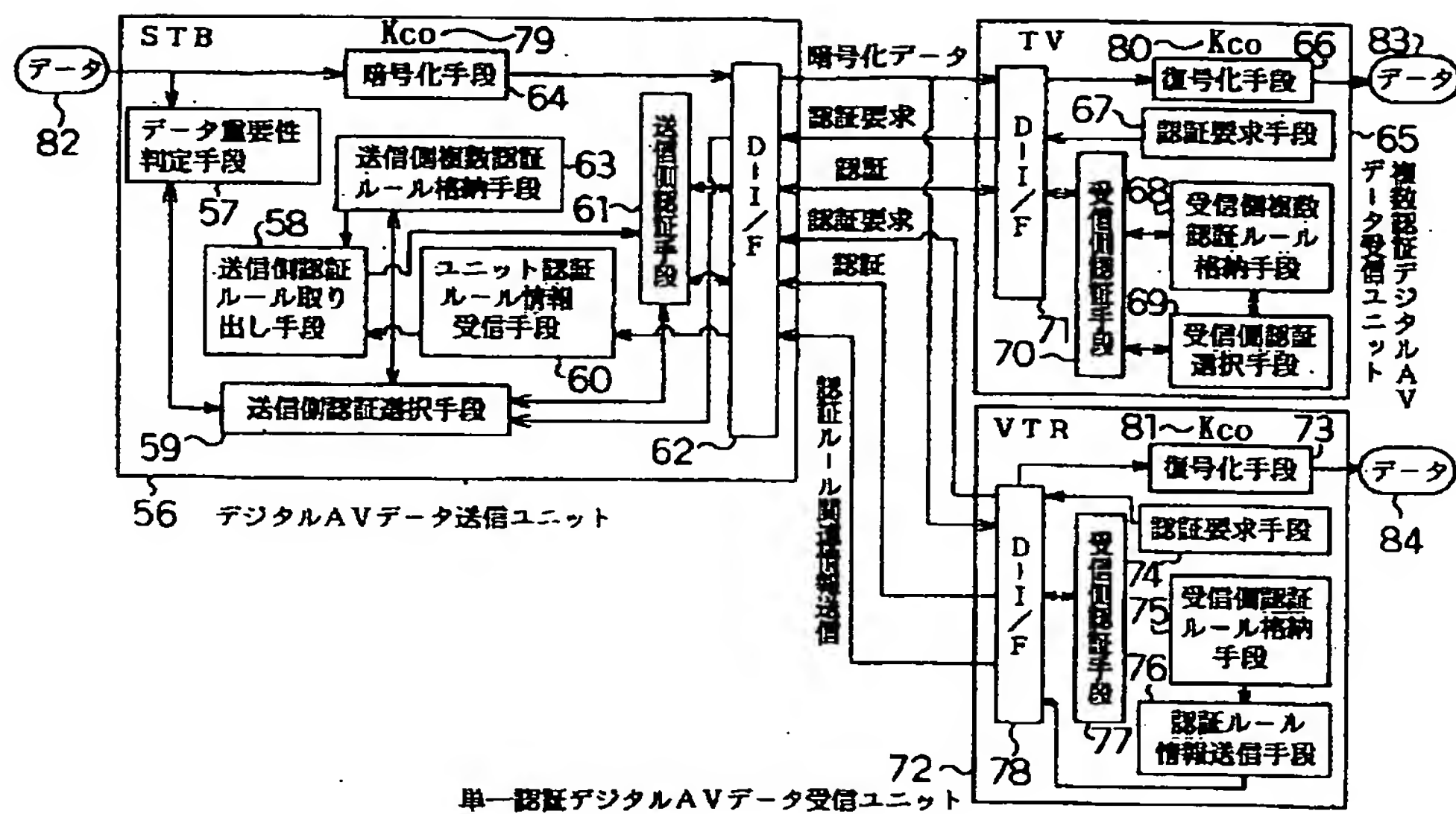
【図6】



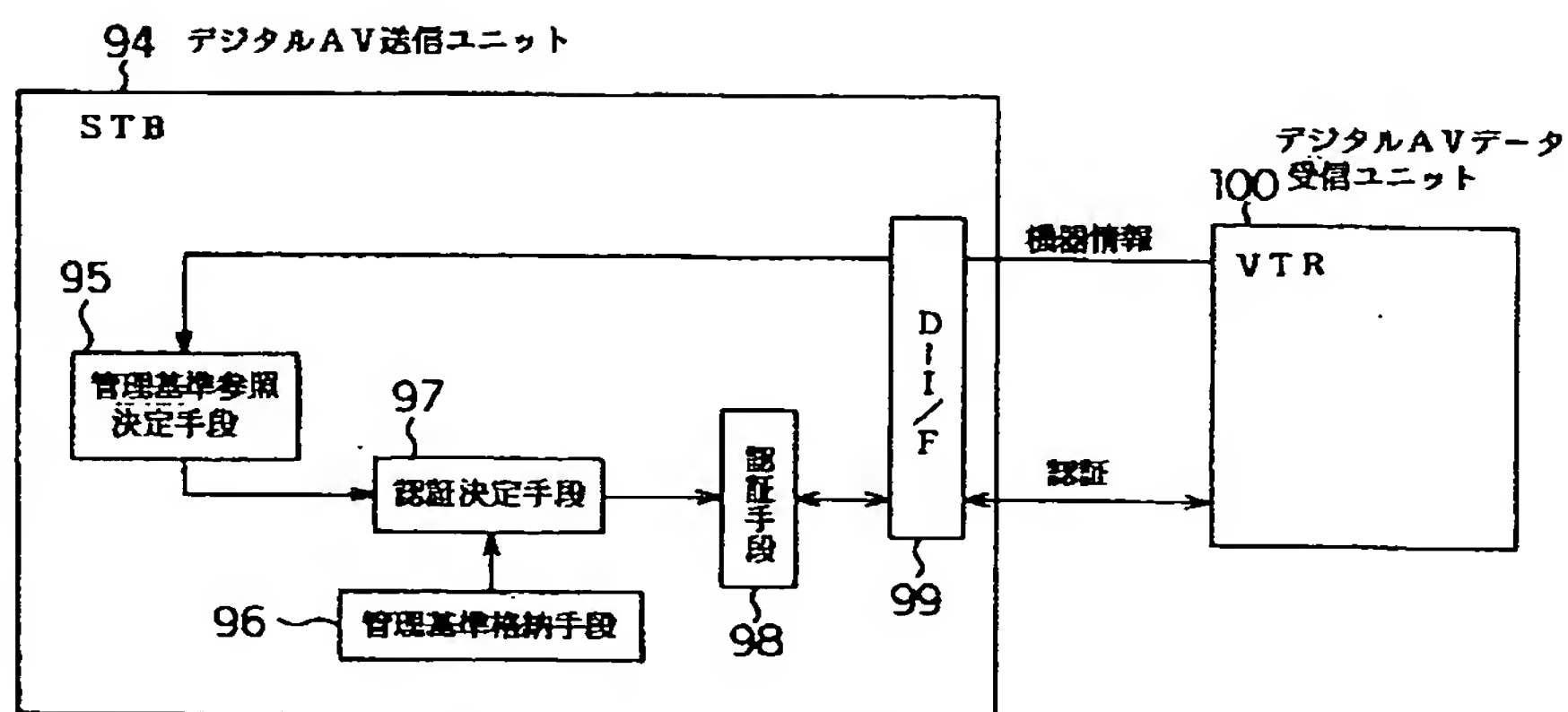
【図8】



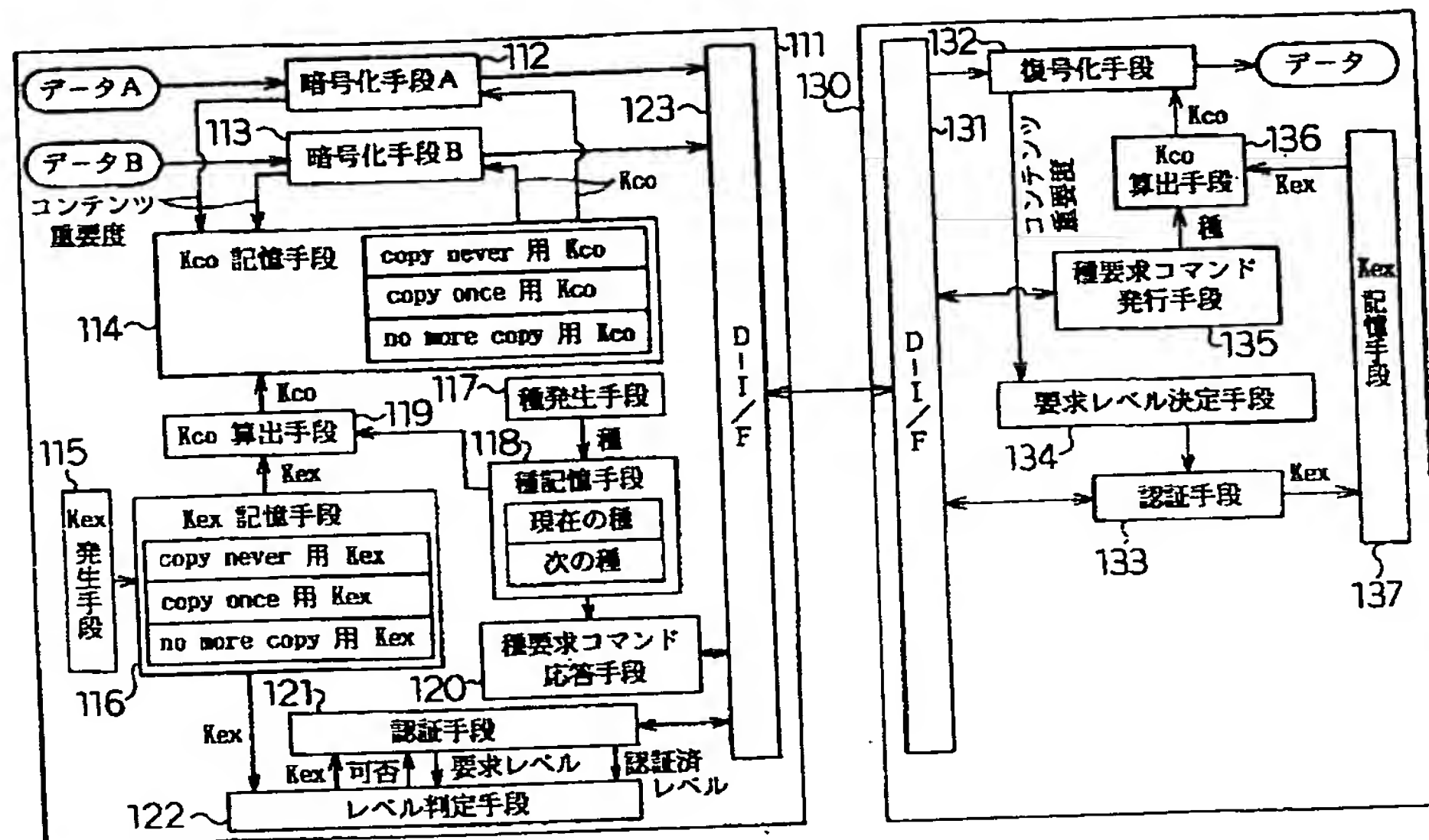
【図7】



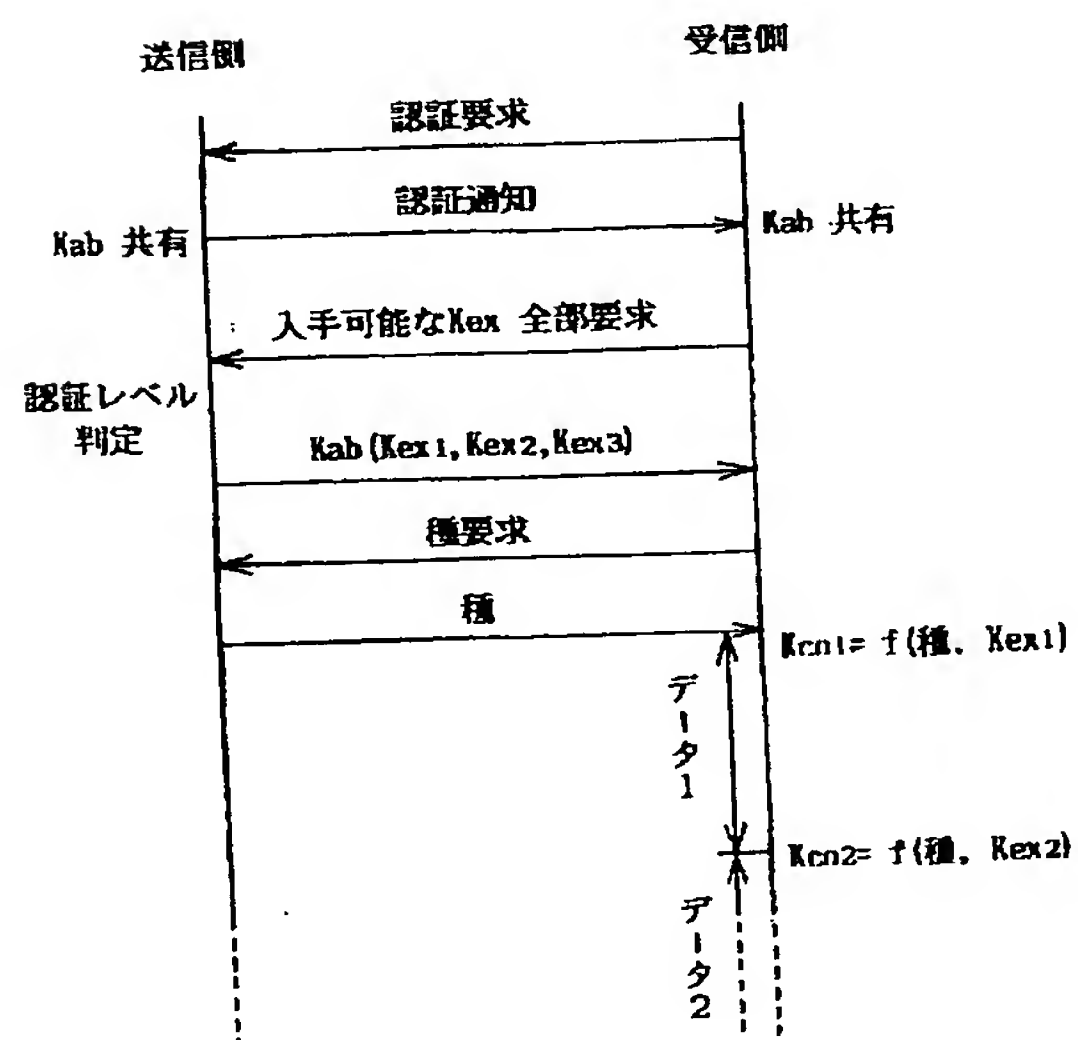
【図9】



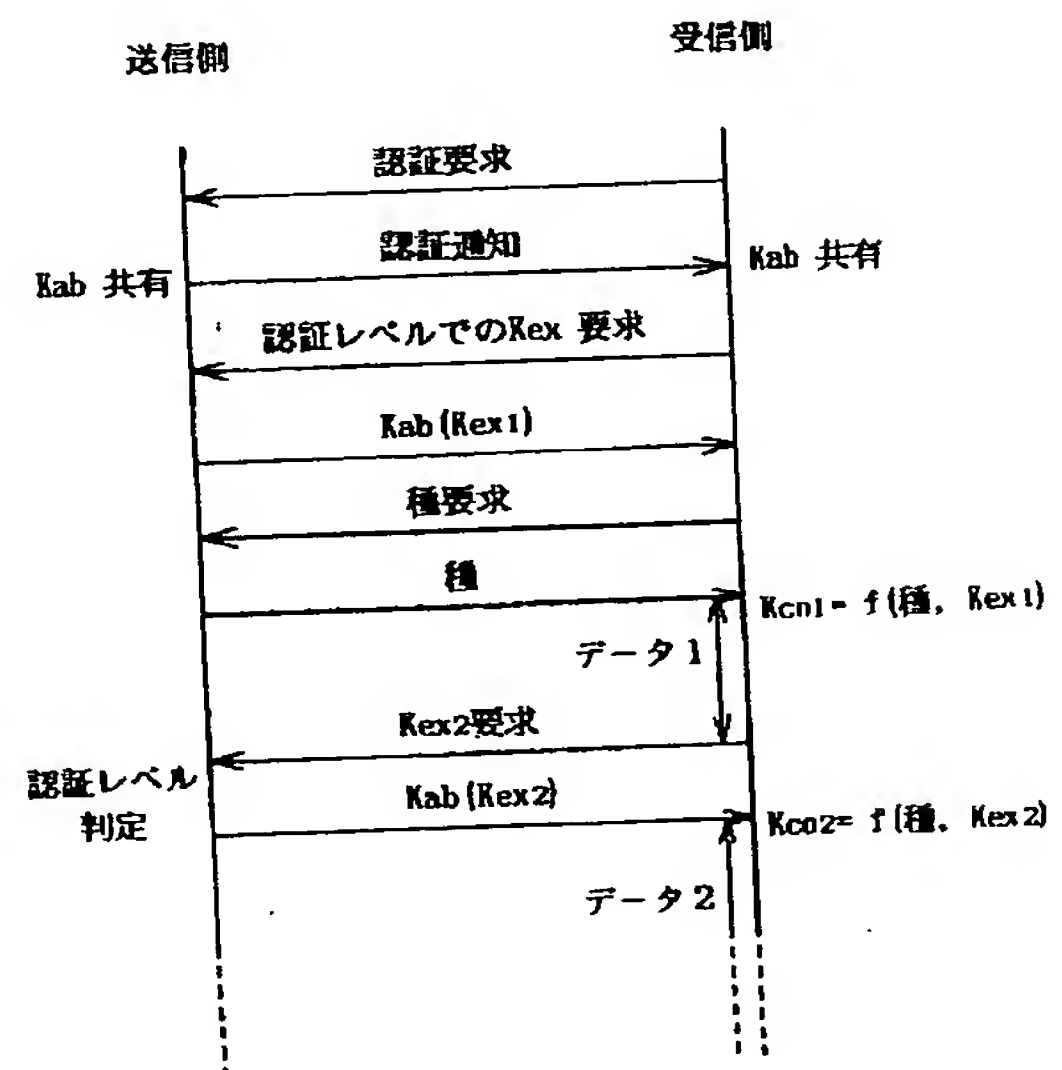
【図10】



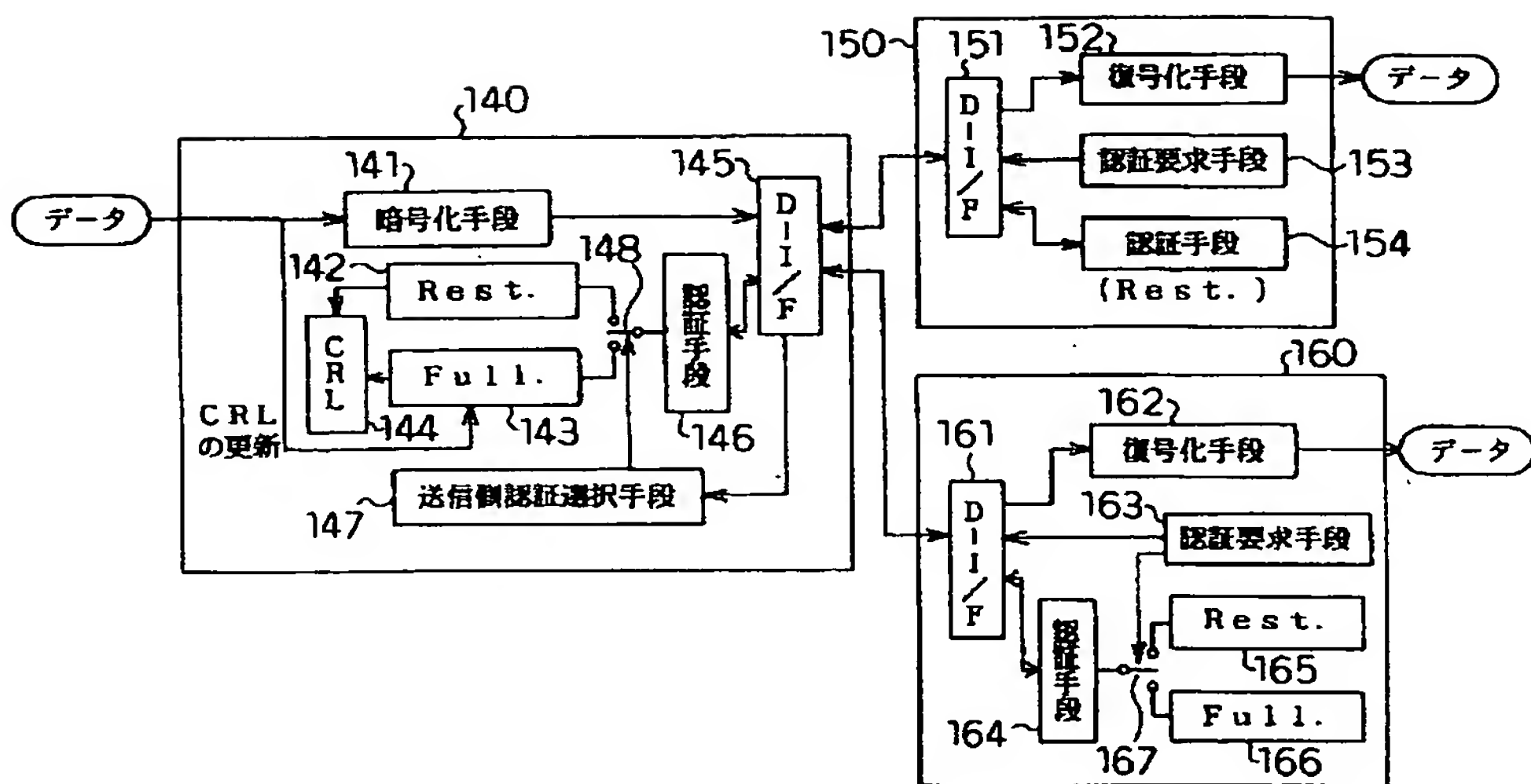
【図11】



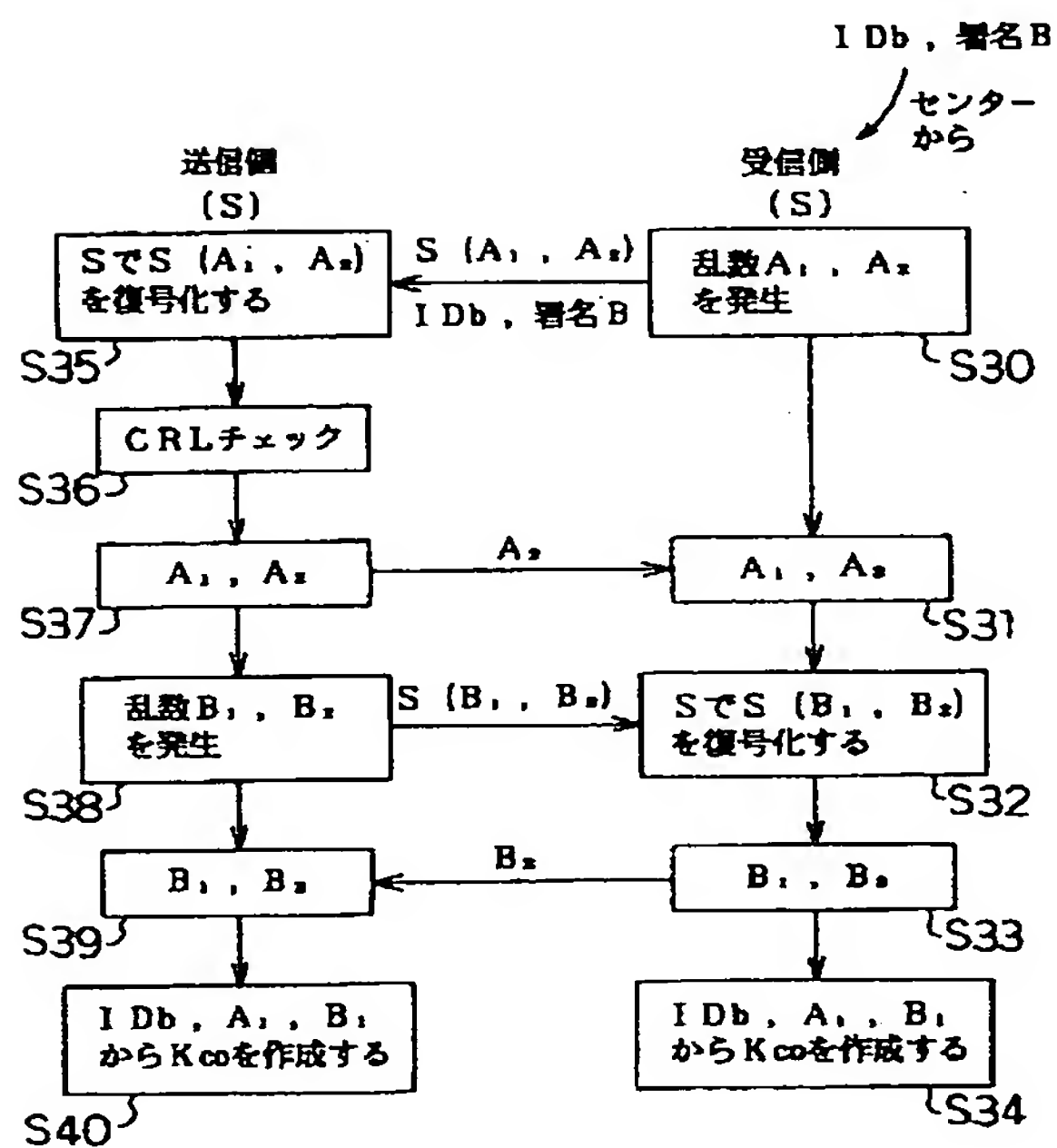
【図12】



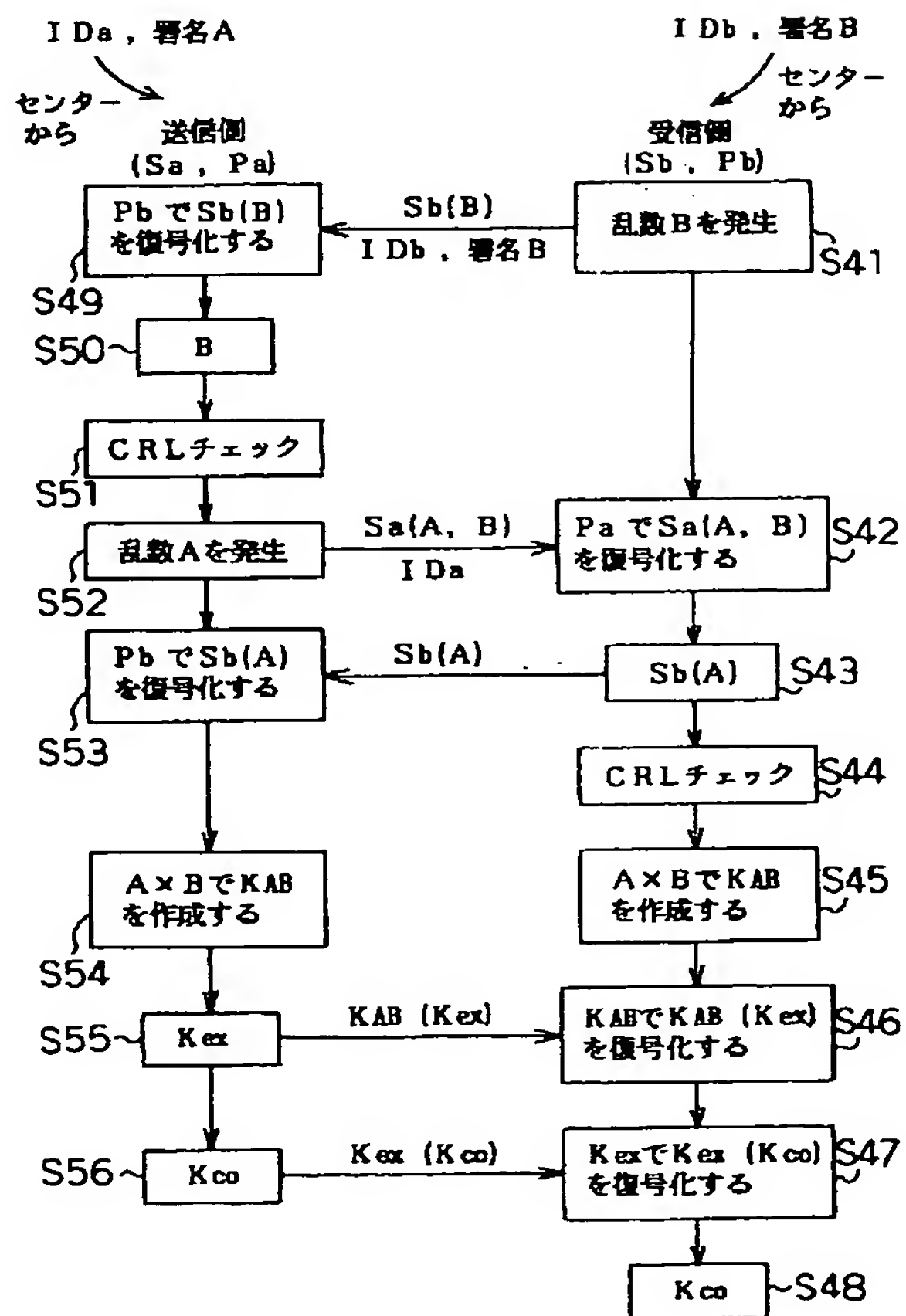
【図13】



【図14】



【図15】



フロントページの続き

(72)発明者 山田 正純
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 後藤 昌一
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 武知 秀明
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 臼木 直司
大阪府門真市大字門真1006番地 松下電器
産業株式会社内